

MATERIAŁY POKONFERENCYJNE



UCZELNIA PAŃSTWOWA
im. Jana Grodka w Sanoku



Redakcja
GRZEGORZ MATYNIAK
WOJCIECH PILSZAK

ZWALCZANIE PRZESTĘPCZOŚCI INTERNETOWEJ

SANOK 2026

ZWALCZANIE PRZESTĘPCZOŚCI INTERNETOWEJ

MATERIAŁY POKONFERENCYJNE

**REDAKCJA
GRZEGORZ MATYNIAK
WOJCIECH PILSZAK**



UCZELNIA PAŃSTWOWA
im. Jana Grodka w Sanoku

SANOK 2026

Wydawca: Uczelnia Państwowa im. Jana Grodka w Sanoku
Redakcja: Grzegorz Matyniak, Wojciech Pilszak
Projekt okładki: Wojciech Pilszak/AI
Korekta językowa: Ewa Indyk
Opracowanie typograficzne: Marcin Stach

© Copyright by
Uczelnia Państwowa im. Jana Grodka w Sanoku
ul. Mickiewicza 21, 38-500 Sanok
www.up-sanok.edu.pl

Poglądy wyrażone w artykułach nie zawsze są zgodne z poglądami Redaktorów i Wydawcy.
Opublikowane referaty nie były poddane korekcie przez Wydawcę i są publikowane w postaci
dostarczonej przez Autorów.

ISBN 978-83-61802-66-2

SANOK 2026

SPIS TREŚCI

Słowo wstępne.....	6
 Paweł Baraniecki	
Czas (nie)jest najprostszą rzeczą	10
 Agnieszka Cenzartowicz, LL.M.	
Poufność jako wektor ataku – o strukturalnym rozdziwieniu między odpowiedzialnością prawnika a kontrolą technologiczną uwag kilka	18
 Józef Druć	
Rzecz o narzędziu do „standaryzacji” analizy i czynności sprawozdawania z oględzin zapisów video lub dokumentacji fotograficznej w prowadzonych postępowaniach.....	24
 Paweł Kaczmarzyk	
Baśnie i legendy o Dysku i Fleszce	39
 Marlena Kruczek	
Wyzwania etyczne w pracy biegłego sądowego – bezstronność czy presja instytucjonalna? .	78
 Wojciech Pilszak	
20 lat funkcji biegłego – historia błędów większych i mniejszych	85
 Marek Stawarczyk	
Analiza nagłówków poczty elektronicznej. Przegląd metod i wybranych narzędzi wspomagających analizę	97
 Tomasz Typrowicz	
Możliwości uzyskiwania oraz analizy danych gromadzonych przez przewoźników lotniczych dotyczących przelotu pasażera (PNR)	123
 Ireneusz Wasiewicz	
Historia sztucznej inteligencji w ujęciu chronologicznym – ludzie, nauka, idee, technologie oraz ich wpływ na społeczeństwa demokratyczne.....	145
 Artur Gałęski, Mateusz Górka	
Kiedy ochrona staje się pokusą – Allegro Ochrona Kupujących z perspektywy bezpieczeństwa platformy	169

Słowo wstępne

Oddawana do Państwa rąk publikacja jest drugą – a niektórzy powiedzieliby, że kolejną – jaka pojawia się po kilkunastu konferencjach organizowanych dla funkcjonariuszy służb państwowych zwalczających przestępczość internetową, czy jak kiedyś mówiono i pisano – komputerową. Czasy się zmieniają, podobnie jak nazewnictwo, ale istota problemu pozostaje ta sama.

Uczelnia Państwowa im. Jan Grodka w Sanoku była w dniach 4–5 września 2025 r. miejscem XVI konferencji przybliżającej zagrożenia związane z użytkowaniem nowoczesnych technologii oraz metod zwalczania działalności przestępczej, której organizatorem był Zakład Bezpieczeństwa Wewnętrznego Instytutu Nauk Społecznych wspólnie z firmą e-Detektywi Sp. z o.o. Tematem przewodnim konferencji było: **Zwalczanie przestępczości internetowej (ZPI)**, która to nazwa po 15 latach zastąpiła wcześniejszą i od roku 2025 będzie znakiem firmowym naszych spotkań, jeżeli oczywiście będzie na nie zapotrzebowanie.

Konferencja – od samego jej powstania – była i jest przeznaczona zgodnie z przyjętymi założeniami dla funkcjonariuszy wszystkich służb mundurowych zajmujących się, w ramach codziennych obowiązków, zwalczaniem zjawiska cyberprzestępczości. Tym razem w murach sanockiej Uczelni pojawiło się 28 prelegentów oraz blisko 220 funkcjonariuszy Policji garnizonu podkarpackiego, placówek Straży Granicznej wchodzących w skład nie tylko Bieszczadzkiego Oddziału Straży Granicznej, ale również innych oddziałów tej formacji w kraju, w tym Wyższej Szkoły Straży Granicznej w Koszalinie. Oczywiście przykładem lat poprzednich nie zabrakło również przedstawicieli Krajowej Administracji Skarbowej z terenu całego kraju, analityków i informatyków śledczych oraz biegłych sądowych z zakresu informatyki śledczej i niezależnych ekspertów z tego zakresu, którzy nieodpłatnie chcieli podzielić się ze słuchaczami swoją wiedzą oraz doświadczeniem.

Prelegentami XVI konferencji byli:

Paweł Baraniecki – ekspert niezależny,

Michał Barbaś – ekspert niezależny,

dr Jarosław Biegański – dyrektor Zespołu Bezpieczeństwa Banków Związku Banków Polskich,

Mateusz Chrobok – ekspert niezależny,

nadkom. Arkadiusz Czak – oficer KAS, Zachodniopomorski Urząd Celno-Skarbowy w Szczecinie,

Józef Druć – emerytowany funkcjonariusz Dolnośląskiego Urzędu Celno-Skarbowego we Wrocławiu, ekspert niezależny,

Mateusz Górka oraz **Artur Gałęski** – Dział ds. współpracy z organami ścigania, Allegro Sp. z o.o.,

Artur Kubiak – emerytowany oficer Policji,

Jakub Kupniewski oraz **Zbigniew Taraś** – Stowarzyszenie Sygnał,

ppor. Tomasz Typrowicz – funkcjonariusz Placówki Straży Granicznej w Sanoku, BiOSG w Przemyśle, biegły sądowy,

Grzegorz Matyniak – emerytowany oficer Policji, biegły sądowy SO w Krośnie z zakresu informatyki śledczej oraz analizy danych, nauczyciel akademicki Uczelni Państwowej im. Jana Grodka w Sanoku,

Jakub Peplowski – ekspert niezależny,

Krzysztof Czarnacki – kierownik Działu Projektów Specjalnych i Administracji Systemów Polkomtel Sp. z o.o.,

Wojciech Pilszak – emerytowany oficer Policji, prezes zarządu e-Detektywi Sp. z o.o., biegły sądowy z zakresu informatyki śledczej i analizy kryminalnej,

Marek Stawarczyk – biegły sądowy z zakresu informatyki i informatyki śledczej SO w Krośnie,

Ireneusz Wasiewicz – ekspert niezależny z zakresu informatyki śledczej,

Tomasz Wawrzakowicz, Mariusz Szmyt – specjaliści ds. współpracy z organami ścigania, Grupa Olx Sp. z o.o.,

Agata Ślusarek – analityk bezpieczeństwa, Departament Cyberbezpieczeństwa KNF,

Jakub Wesołowski – ekspert niezależny,

Wojciech Bulanowski – Żandarmeria Wojskowa w Krakowie,

Paweł Kaczmarzyk – prezes firmy Kaleron Sp. z o.o.,

Mateusz Sabaj – Netia SA,

Ewelina Wojciechowska – analityk kryminalny, Prokuratura Okręgowa w Katowicach,

Artur Wojciechowski – Dyrektor Centrum Cyberbezpieczeństwa WSIiZ w Rzeszowie,

Agnieszka Cenzartowicz – SWC Group.

Celem konferencji, jak założono od samego początku, było i jest nadal praktyczne poszerzenie wiedzy z zakresu szeroko pojętej cyberprzestępczości oraz jej zapobiegania przez funkcjonariuszy różnych służb na co dzień zmagających się z tą formą rozwijającej się dynamicznie działalności przestępczej.

Wśród wystąpień nie zabrakło tematów opartych na faktycznych przypadkach działalności przestępczej i to te wystąpienia są najbardziej oczekiwane przez uczestników konferencji, są solą przekazywanej wiedzy. Poruszono tematy dotyczące możliwości technicznych i prawnych zabezpieczania danych stanowiących lub mogących stanowić dowód w prowadzonych postępowaniach karnych, co jest niezwykle istotne z punktu widzenia organów ścigania, których przedstawiciele corocznie są obecni konferencji.

Prelegenci poruszali również tematy związane z wykorzystywaniem narzędzi informatycznych pozwalających na analizę i obróbkę zarówno materiałów wideo, zdjęć ale też danych telemetrycznych zabezpieczanych w ramach prowadzonych postępowań przygotowawczych i ich procesowego wykorzystania. Przykładem tego ostatniego zagadnienia było wystąpienie Jakuba Wesołowskiego dotyczące danych telemetrycznych, jakie można pozyskać z urządzeń mobilnych.

Po raz kolejny nowości we współpracy sektora bankowego z organami ścigania przedstawił Jarosław Biegański, dyrektor Zespołu Bezpieczeństwa Banków Związku Banków Polskich. Rąbka swojego warsztatu pracy uchylili biegli sądowi z zakresu informatyki śledczej biorący udział w konferencji.

Interesującym wystąpieniem był temat związany z oprogramowaniem dotyczącym transkrypcji mowy bez dostępu do sieci wykorzystującym modele AI do lokalnej transkrypcji audio o nazwie Whisper Offline, na potrzeby prowadzonych czynności procesowych, jak i operacyjno-rozpoznawczych, które pozwalają zaoszczędzić czas. Narzędzie to przedstawił nadkomisarz Arkadiusz Czak – człowiek, który nigdy nie odmówił nikomu pomocy, kto zwrócił się do niego z tego rodzaju problemami.

Zasygnalizowano w szerszym zakresie sposoby wykrywania urządzeń podsłuchowych, ukrytych urządzeń dostępowych, kamer oraz urządzeń GSM, które przedstawił Józef Druć, emerytowany ekspert KAS. Co ważne nie były to metody do których wykorzystuje się specjalnie drogie urządzenia ale takie, które mogą być nabyte w ramach posiadanych niewielkich funduszy.

Ewelina Wojciechowska, biegła z zakresu analizy kryminalnej, wskazała na zasadność tworzenia stanowisk specjalistycznych w strukturach organów ścigania czego przykładem okazały się stanowiska odczytu urządzeń mobilnych uruchomione w Prokuraturze Okręgowej w Katowicach.

Nie brakowało też zagadnień dotyczących sztuki manipulacji w erze Internetu czyli wszelkiego rodzaju kłamstw, oszustw i gry na emocjach ofiar, jakie są stosowane ze strony sprawców cyberprzestępstw, który to temat bardziej ciekawie przedstawił Ireneusz Wasiewicz. Czekamy na kolejne tego rodzaju intrygujące wystąpienia. Artur Wojciechowski usiłował przekonać – być może się to udało – że temat naruszeń prawa autorskiego w sieci w kontekście utworów literackich nie odszedł jeszcze w niepamięć.

Trendy nowych pomysłów, jakie pojawiły się ze strony sprawców, ale – co ważne – przeciwdziałania tymże wskazali pracownicy Olx i Allegro, dając nadzieję, że jednak klienci nie są pozostawiani sami sobie. Ze strony Agnieszki Cenzartowicz miało miejsce bardzo ciekawe i co ważne – życiowe – ukazanie problemów, jakie dotyczą tzw. love scamów. Mam tu na myśli zarówno problemy ofiar, ale również problemy jakie niejednokrotnie generują sami przedstawiciele organów ścigania.

To tylko niektóre z bardzo ciekawych wystąpień jakich wysłuchać mogli uczestnicy konferencji.

Na koniec, jak corocznie pojawiają się pytania – czy sanockie spotkania ekspertów ze służbami nadal będą trwały? A jeżeli tak to w jakiej formie? Czy jest na nie jeszcze zapotrzebowanie? Te pytania – pojawiające się za każdym razem, kiedy zbliża się kolejna edycja konferencji – pozwolą Państwo, pozostawię na tę chwilę bez odpowiedzi. Chociaż zwiększająca się z każdym rokiem liczba uczestników – zarówno w postaci ekspertów, ale co równie istotne uczestników, słuchaczy – zdaje się przynosić na te pytania odpowiedź sama.

Konferencja, co widać na przestrzeni czasu, a w szczególności od roku 2025 ewoluuje – dziękuję Ci Wojtku – i nie jest i nigdy nie będzie zamknięta dla przedstawicieli żadnego z organów ścigania i innych służb, które stykają się z tymi problemami i będą się chciały dzielić doświadczeniem i wiedzą z innymi. Dotyczy to również prelegentów z sektora prywatnego i im również dziękuję za nieodpłatnie poświęcony czas.

W tym miejscu po raz kolejny (i nieustający) chciałbym złożyć swoje podziękowania tym wszystkim, którzy przez cały okres trwania mojego pomysłu pojawili się w Sanoku i nigdy –

co niezwykle istotne – nie odrzucili skierowanego do nich z mojej strony zaproszenia. I na których pomoc – co też ważne – mogłem i mogę liczyć nadal.

Mamy rok 2026 i pomimo padających kiedyś z mojej strony zapowiedzi, że XV edycja będzie ostatnią, zbliża się nasze XVII spotkanie – a może nawet będą Państwo na tym spotkaniu, które odbędzie się w dniach 27–28.08.2026 r. i nadal się spotykamy? Co ciekawe konferencja po raz pierwszy w swojej historii będzie odbywać się w dwóch sesjach równoległe, powrócą warsztaty praktyczne – nie wiem czy są z nami jeszcze słuchacze, którzy pamiętają, że takowe się odbyły oraz po raz pierwszy będzie z nami aż 41 prelegentów. Wygląda na to, że dzięki namowom takich samych pozytywnie zakręconych osób (wiecie, że to o Was), po poszerzeniu grona odbiorców mogących skorzystać z wiedzy i doświadczenia innych (przy zachowaniu tych samych kryteriów udziału, przepraszam, jeżeli niektórych tym do siebie zraziłem, ale to się nie zmieni) oraz przy nieco innej formie docierania do coraz szerszej grupy zainteresowanych, to cykliczne wydarzenie na sanockiej Alma Mater na stałe jest obecne na mapie działalności na rzecz cyberbezpieczeństwa Polski. Czy jest ono istotnym i ważnym dla słuchaczy miejscem spotkań, wymiany doświadczeń ekspertów, biegłych sądowych, funkcjonariuszy służb mundurowych, pracowników sektora prywatnego, którzy zajmują się bezpieczeństwem użytkowników cyberprzestrzeni? Ilość uczestników, których z każdym rokiem przybywa wskazuje na to bezdyskusyjnie.

Życząc Państwu miłej lektury zachęcam do kontaktu z redaktorami w sprawie kolejnych spotkań i kolejnych – mam taką nadzieję – monografii.

Z wyrazami szacunku,
podziękowaniami
i życząc miłej lektury

Grzegorz Matyniak

Czas (nie)jest najprostszą rzeczą

Abstrakt

W niniejszym opracowaniu wykazano konieczność ustalenia źródła wzorca, zestawu atrybutów zapisów czasu w logach, czy metadanych, tak aby przez ich konwersję na czas urzędowy zbudować chronologię zdarzeń będących przedmiotem analizy w postępowaniu.

This study demonstrates the need to determine the source of the pattern, a set of attributes of time records in logs, or metadata, so that by converting them into official time, a chronology of events that are the subject of analysis in the proceedings can be built.

Wstęp

Czas, a zwłaszcza jego pomiar był ważny od starożytności. Od czasu Wielkich Odkryć Geograficznych (XV wiek) pomiar czasu stał się istotny w nawigacji dla prawidłowego wyznaczania długości geograficznej. Skokowy wzrost wymagań dla dokładności pomiaru czasu przyniósł telegraf. Zawierano transakcje, których rozliczenie wymagało jednolitej podstawy czasowej. Coraz większa szybkość komunikacji wymagała coraz dokładniejszego wyznaczania czasu. Ustalono wzorzec jednostki czasu (sekunda), a nieco później strefy czasowe i czas wzorcowy mierzony na południku 0 (czas Greenwich, czas uniwersalny).

Oznaczenie czasu wystąpienia danego zdarzenia pozwala na:

- wyznaczenie chronologii zdarzeń;
- wnioskowaniu o związkach pomiędzy zdarzeniami typu przyczyna i skutek.

Aby to było możliwe należy posługiwać się czasem wyznaczonym przez wzorzec, bądź o znanej różnicy pomiędzy czasem wzorcowym, a czasem zapisanym w logach, czy metadanych.

Czas – podstawowe terminy

Definicje

W każdym państwie jest określony czas urzędowy. W Polsce czas urzędowy jest określony ustawą¹, a jego definicja jest następująca:

„Art. 2.

1. Czasem urzędowym na obszarze Rzeczypospolitej Polskiej jest czas środkowoeuropejski albo czas letni środkowoeuropejski w okresie od jego wprowadzenia do odwołania.
2. Czas środkowoeuropejski jest czasem zwiększonym o jedną godzinę w stosunku do uniwersalnego czasu koordynowanego UTC(PL).
3. Czas letni środkowoeuropejski jest czasem zwiększonym o dwie godziny w stosunku do uniwersalnego czasu koordynowanego UTC(PL).
4. Uniwersalny czas koordynowany UTC(PL) jest polską realizacją międzynarodowego uniwersalnego czasu koordynowanego UTC i wyznaczany jest przez państwowy wzorzec jednostek miar czasu i częstotliwości”.

¹ Ustawa z dnia 10 grudnia 2003 r. o czasie urzędowym na obszarze Rzeczypospolitej Polskiej (Dz. U. z 2004 r., nr 16 poz. 144).

Zaś uniwersalny czas skoordynowany UTC, to:

„wzorzec ustalany na podstawie wskazań zegara atomowego i koordynowany przez czas słoneczny”.

Oznacza to, że w każdym roku wprowadzana jest poprawka. Jak dotąd dodawane są poprawki nie przekraczające 1 sekundy.

Wzorce czasu

W sieci jest wiele serwisów przedstawiających czas według różnych wzorców. W poniższej tabeli nr 1 podano zestawienie dwóch najczęściej używanych wzorców²:

local	2025-10-21 16:14:33	Tuesday	day 294
UTC	2025-10-21 14:14:33	Tuesday	day 294
GPS	2025-10-21 14:14:51	week 2389	224091 s

Tabela nr 1. Zestawienie wybranych wzorców czasu.

Czas oznaczony jako „local” jest czasem na komputerze autora.

UTC to czas środkowoeuropejski, co roku koordynowany względem czasu słonecznego. Obowiązuje on na długości geograficznej 0 (Południk Greenwich). Czas lokalny w innych miejscach będzie się różnił o jakąś ilość godzin. W Polsce – zależnie od pory roku – jest on późniejszy o jedną (czas zimowy) lub dwie godziny (czas letni).

GPS to czas obowiązujący w satelitach systemu nawigacyjnego GPS³. Jest on niezmienny od czasu włączenia w czerwcu 1980 roku. Dlatego „wyprzedza” on czas UTC, do którego co roku wprowadza się poprawkę.⁴

W roku 2025 różnica pomiędzy czasami wzorców GPS, a UTC wynosi 18 sekund. W kolejnych latach ta różnica może być inna.

Kto automatycznie synchronizuje czas ze wzorcem?

Odpowiedź lapidarna: stosują Ci, którzy muszą, lub im się opłaca. W pierwszej grupie tych, którzy muszą są:

- urzędy i administracja;
- użytkownicy urządzeń podłączonych do Internetu. Systemy operacyjne komputerów, czy smartfonów i wielu urządzeń IOT domyślnie synchronizują czas ze wzorcem. Uwaga:
 - to ustawienie można zmienić,
 - komputery należące do firm globalnych mogą synchronizować czas z czasem obowiązującym w centrali danej firmy.

W drugiej grupie (tym, którym się opłaca) są:

- dostawcy usług:
 - zaufania publicznego (stempel czasowy itp.),
 - powszechnych (energia, telekomunikacja...),
 - transport,

² Źródło: <http://leapsecond.com/java/gpsclock.htm> [dostęp: 21-10-2025].

³ Global Positioning System.

⁴ Od czasu uruchomienia GPS nie było ujemnych poprawek czasu UTC.

- instytucje finansowe.

W tych dziedzinach dla celów wzajemnych rozliczeń, tak między organizacjami, jak i między osobami i organizacjami konieczne jest używanie czasu synchronizowanego z wzorcem.

Kto nie synchronizuje automatycznie czasu ze wzorcem?

Kolejna odpowiedź lapidarna: ci, którzy nie mogą, lub nie chcą. Nie mogą automatycznie synchronizować czasu na urządzeniach niepodłączonych do Internetu, np.:

- kamery, także rejestratory samochodowe i aparaty fotograficzne;
- monitoring wizyjny (CCTV itp.);
- zegarki i zegary elektroniczne.

Zaś w grupie celowo odłączonych od Internetu urządzeń można znaleźć:

- używane samochody (zwłaszcza marek premium);
uniemożliwia to żądania wizyt w autoryzowanym warsztacie;
- Czytniki e-booków;
osób niekorzystających z „bibliotek w chmurach”.
- Smartfony opanowane przez malware;
często łączone w grupy, mają czas urządzenia „master”.

Zapis daty i czasu

Wiele urządzeń elektronicznych zapisuje datę i czas danego zdarzenia. Czas danego wydarzenia może być zapisany na różne sposoby. Sposób zapisu daty i czasu jest (najczęściej) skonfigurowany w systemie operacyjnym, bądź firmware urządzenia.

Zapis daty

Sposoby zapisu daty różnią się:

- kolejnością zapisu dnia, miesiąca i roku;
 - format amerykański: miesiąc, dzień, rok; np. 10/11/2025,
 - format brytyjski: dzień, miesiąc, rok; np. 11-10-2025,
 - format zgodny z normą ISO 8601: rok, miesiąc, dzień; np. 2025-10-11
- długością zapisu tekstowego nazw miesiąca i roku.

Stosowane są trzyliterowe skróty nazw miesięcy i zapisywanie dwóch ostatnich cyfr roku np. 11 paź 25⁵.

Urządzenia elektroniczne zapisują datę danego zdarzenia najczęściej w postaci ciągu cyfr.

Typowy błąd odczytu daty

Przy zapisie daty w postaci ciągu cyfr jak w przykładzie: 10/11/2025 może to oznaczać 11 października 2025 roku (wg formatu amerykańskiego) lub 10 listopada 2025 roku (wg formatu brytyjskiego). Bez rozpoznania stosowanego na danym urządzeniu formatu zapisu daty można popełnić poważny błąd.

⁵ Występują też kombinacje z tekstowym zapisem nazwy dnia, a także pełnych nazw miesięcy.

Zapis czasu

Dla jasności wyводу zajmijmy się najczęściej spotykanym zapisem czasu w postaci cyfr:

gg:mm:ss,xxx

gdzie:

gg – godzina (2 cyfry),

mm – minuty (2 cyfry)

ss,xxx – sekundy z dokładnością do tysięcznej⁶.

Przy stosowaniu tego zapisu są wykorzystywane atrybuty.

Atrybuty zapisu czasu

Użytkownik może dowolnie ustawić atrybuty zapisu czasu na swoim urządzeniu. W efekcie, zapisany czas może być znacząco inny od obowiązującego w miejscu zdarzenia czasu urzędowego przypadającego na ten moment.

Strefa czasowa

W zależności od długości geograficznej obowiązują różne strefy czasowe. W pewnym przybliżeniu⁷, na każde 15° długości geograficznej przypada 1 godzina różnicy w stosunku do wzorca UTC.

Czas letni/zimowy

Co pół roku w wielu państwach jest zmieniany o 1 godzinę czas urzędowy. W logach godzina w chwili zmiany czasu jest zaznaczana literą „a”. Zmiana czasu z letniego na zimowy następuje o godzinie 03:00:00, kiedy „staje się” ona godziną 02a:00:00. Zlekceważenie w analizie danych litery „a” doprowadzi do nieuchronnego błędu.

Zapis 12- lub 24-godzinny

Godzina 22 w zapisie 12-godzinnym będzie przedstawiona (zależnie od urządzenia) jako:

> 10 pm

> 10.

> 10

Zaniechanie ustalenia sposobu zapisu czasu uniemożliwi odróżnienie godziny np. 21 od 9.

W praktyce

Metadane pliku graficznego (zdjęcia)

Prezentowane tu zdjęcie flaminga jest zrobione w pogodny, słoneczny dzień. Położenie światła i cieni wskazuje na czas wykonania zdjęcia przed południem lub wczesnym popołudniem. Tymczasem z metadanych tego zdjęcia (patrz grafika nr 1) wynika, że zdjęcie wykonano o 22:46.

⁶ Może być stosowana inna dokładność pomiaru, np. do setnej.

⁷ Z przyczyn gospodarczych i/lub politycznych obszar obowiązywania danej strefy czasowej może być zmieniony, np. w Chinach obowiązuje tylko jedna strefa czasowa.



Fot. nr 1. Zdjęcie autora

File Information	
File:	DSC_1302.JPG
Located in:	
Type:	ACDSee Ultimate 2025 JPEG Image
Size:	1,8 MB
Created:	11.12.2017 18:45
Modified:	11.12.2017 18:45
Accessed:	09.08.2025 15:44
☐ Read Only	☐ Hidden
Image Attributes	
Image Dimensions:	2680 x 4016 (10.8 MP)
Uncompressed Size:	30,8 MB
Bit-Depth:	24-bit color
Pages:	1 page(s)
Pixels Per Inch:	300
Image Dimensions (in)	8.93 x 13.39
Embedded Color Profile:	sRGB IEC61966-2.1
EXIF metadata (summary):	
Model	NIKON D610
Shutter Speed	1/2000 s
F-Number	f/5.6
ISO	ISO 320
Exposure Bias Value	0.00 eV
Metering Mode	Pattern
Flash	Off. Did not fire
Focal Length	340 mm
Date/Time Original	27.11.2017 22:46

Grafika nr 1. Metadane fotografii nr 1

Ta sprzeczność wynika z ustawienia na aparacie czasu obowiązującego w Polsce, a zdjęcie wykonano w innej, dalekiej strefie czasowej.

W przedstawionym przykładzie rozbieżność jest łatwo wytłumaczalna. Ale w przypadku zdjęcia zrobionego przy świetle sztucznym, lub w przestrzeni zamkniętej bez analizy danych typu: model kamery, parametry naświetlania do zapisu czasu utworzenia pliku należy podchodzić z dużą nieufnością.

Film z rejestratora samochodowego i innych kamer

Popularny element wyposażenia samochodów. Nagrania z rejestratora często są badane pod kątem przydatności dowodowej.

Pierwszymi pytaniami są: kiedy i gdzie nagrane zdarzenie miało miejsce? O ile nagranie nie było robione na środku oceanu lub pustyni to ustalenie miejsca (w większości przypadków)

nie powinno być trudne. Za to ustalenie urzędowego czasu nagranych zdarzeń może narażać na trudności i być obciążone błędem.

W praktyce spotykamy nagrania z dedykowanych rejestratorów, kamer sportowych (najczęściej motocykliści) i smartfonów, w których nagraniami zarządza aplikacja do nawigacji, czy ostrzegania przed pomiarem prędkości lub miejscami niebezpiecznymi. Na nagraniu mogą być dodane informacje o dacie i czasie, prędkości położeniu geograficznym. Ale nie muszą.

W każdym przypadku należy ustalić jaki czas obowiązuje na urządzeniu z którego pochodzi nagranie. Czyli należy ustalić:

1. Czy urządzenie synchronizuje czas ze wzorcem, a jeśli tak, to z którym?

Instrukcja obsługi rejestratora dostarczy informacji czy urządzenie może synchronizować czas i z jakim wzorcem. W wielu rejestratorach czas jest synchronizowany ze wzorcem GPS. W przypadku, gdy rolę rejestratora pełni smartfon należy ustalić, czy a nagraniu dodawany jest czas według wzorca GPS, czy UTC.

Nie można zapomnieć o różnicy pomiędzy czasami wskazywanymi przez wzorce GPS i UTC. W 2025 roku różnica ta wynosi 18 sekund.

Przez 18 sekund, przy prędkości 50 km/h pojazd przejedzie ok. 250 metrów. Przy porównaniu nagrań z monitoringu miejskiego (czas według UTC) z nagraniami z rejestratora (czas w GPS) brak uwzględnienia tych 18 sekund różnicy doprowadzi do poważnego błędu.

2. Jakie atrybuty zapisu czasu ustawiono na urządzeniu (strefa czasowa, czas letni/zimowy, zapis 12/24 godzinny)?

Należy ustalić jakie atrybuty zapisu czasu są ustawione w rejestratorze.

Na podstawie ustaleń będzie można wyznaczyć różnicę (poprawkę) pomiędzy czasem urzędowym, a czasem zapisywanym przez rejestrator.

Rejestratory nie synchronizujące czasu

W takim przypadku należy sprawdzić jaki czas i przy pomocy jakich atrybutów jest zapisywany przez urządzenie. Do wstępnej analizy za wzorec czasu urzędowego może służyć smartfon, który pobiera czas z sieci operatora telekomunikacyjnego.

Zdarza się, że w rejestratorach pracujących dłuższy czas akumulator już nie działa, a urządzenie jest wzbudzone, gdy dostanie napięcie z instalacji elektrycznej samochodu. W takich przypadkach czas zaczyna być mierzony za każdym startem silnika od „czasu początkowego” firmware urządzenia np. od 01-01 2002 godz. 00:00.

Rejestratory nie zapisujące czasu na nagraniu

W takim przypadku należy z metadanych pliku nagrania odczytać czas jego utworzenia i zmierzyć czas jaki upłynął od utworzenia pliku do interesującego nas nagrania. Nie można zaniedbać ustalenia jaki czas jest ustawiony na urządzeniu, by móc ustalić czas urzędowy utworzenia pliku z nagraniem.

Inne kamery

Tak samo należy postępować z nagraniami filmów ze smartfonów, systemów lub pojedynczych kamer monitoringu.

Urządzenia, które nie synchronizują czasu ze wzorcem

Każdy pomiar, także i czasu jest obarczony błędem. Wskazania czasu na urządzeniu, czy w sieci, które nie synchronizują czasu będą zależać od błędu pomiaru czasu i daty ostatniej jego regulacji. Przy długim odstępie czasu od ostatniej regulacji może dochodzić błąd braku uwzględnienia sezonowej zmiany czasu (letniego na zimowy, lub odwrotnie). Taka sytuacja często występuje w samochodach już po gwarancji.

W takim przypadku należy, oprócz ustalenia ustawienia atrybutów zapisu czasu, wyznaczyć poprawkę pomiędzy czasem wskazywanym przez urządzenie, a czasem np. smartfona, czy innego urządzenia synchronizującego czas.

Czas w poczcie elektronicznej

Wielokrotnie akta sprawy zawierają wydruki listów poczty elektronicznej. Na wydruku widać kto, do kogo, kiedy wysłał informację i treść tej informacji. Tak dokumentuje się przekazanie informacji od nadawcy do odbiorcy, jak i czasu kiedy to przekazanie miało miejsce. Jeżeli wydruk nie zawiera pełnego nagłówka e-maila to nie można ufać czasowi jaki widnieje na wydruku. Wykażę to na przykładzie mojej korespondencji.

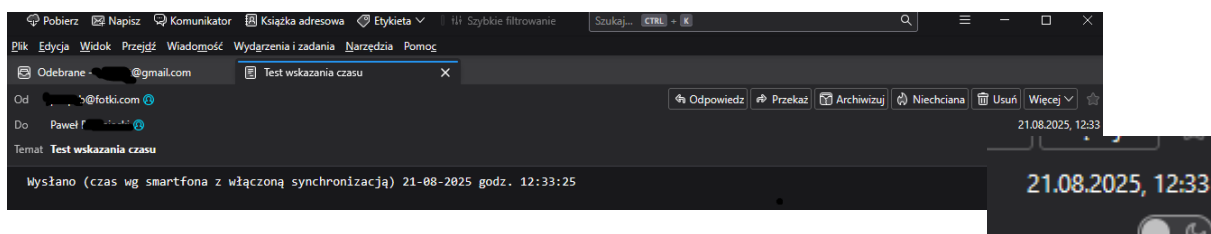
Wysłałem e-maila z mojej skrzynki w domenie @fotki.com (dostęp przy pomocy przeglądarki Mozilla Firefox) na drugi mój adres poczty elektronicznej w domenie @gmail.com (dostęp przy pomocy programu klienta pocztowego Mozilla Thunderbird).

List wysłałem 21 sierpnia 2025 o godz. 12:23:25 (czas według mojego smartfona synchronizującego czas z siecią operatora telekomunikacyjnego). Przedstawiam zrzuty z Firefox i Thunderbird.



Grafika nr 2. Widok listu w domenie @fotki.com (przeglądarka Firefox)

Powiększono czas wysłania i dostarczenia



Grafika nr 3. Widok listu w domenie @gmail.com (Thunderbird). Powiększono czas dostarczenia

Jak widać czas dostarczenia różni się o 6 godzin. Z którego narzędzia wydruk (przeglądarka, klient poczty elektronicznej) załączyć do akt?

Wydruk każdego z przedstawionych widoków nie może dostarczać informacji o czasie wysłania. Aby uwiarygodnić czas wysłania wydruk musi przedstawiać pełny nagłówek listu, w którym widać każdy etap jego drogi. Czasy w takim nagłówku są prezentowane w odniesieniu do wzorca UTC i stref czasowych.

Wy tłumaczenie pokazanej rozbieżności czasowej jest proste. Domena @fotki.com w dniu pisania listu miała czas UTC -04:00 (EDT wschodnioamerykański czas letni), a w Polsce obowiązywał wtedy czas letni UTC +02:00. Różne strefy czasowe są przyczyną pozornej rozbieżności.

Podsumowanie

W sprawach, w których istotny jest czas zdarzeń należy czasy zapisane w logach, czy metadanych skonwertować do czasu urzędowego. Jako wzorzec czasu urzędowego, często z wystarczającą dokładnością, może służyć smartfon lub smartwach pobierający czas z sieci operatora telekomunikacyjnego. Zawsze należy sprawdzić:

- Jakie atrybuty zapisu czasu są ustawione na urządzeniach?
- Czy choć jedno urządzenie synchronizuje czas ze wzorcem, jeśli tak, to z którym?

To pozwoli na wyznaczenie dla każdego urządzenia różnicy pomiędzy czasem wskazywanym, a czasem wzorcowym. Później, korzystając z wyznaczonych różnic, można dokonać konwersji czasu danego urządzenia na czas urzędowy. Zasady te obowiązują dla wszystkich urządzeń, które dokonują pomiaru czasu i jego zapisu.

Posługiwanie się czasem urzędowym i oszacowanie błędu pomiaru czasu jest szczególnie istotne w przypadkach pobierania danych od operatorów telekomunikacyjnych, banków, czy usługodawców usług świadczonych elektronicznie. W tym ostatnim przypadku należy prosić o informację o synchronizacji czasu.

Agnieszka Cenzartowicz, LL.M.

Poufność jako wektor ataku – o strukturalnym rozdźwięku między odpowiedzialnością prawnika a kontrolą technologiczną uwag kilka

Abstrakt

Artykuł analizuje fundamentalny rozdźwięk między koncentracją odpowiedzialności prawnej po stronie prawnika jako administratora danych a rozproszoną kontrolą nad infrastrukturą techniczną sprawowaną przez dostawców IT. Punktem wyjścia jest incydent spoofingu domeny kancelarii, który odsłania problem systemowy: prawnik odpowiada za skutki naruszeń bezpieczeństwa, ale często nie ma wpływu na konfigurację systemów, tempo reakcji ani dostęp do informacji niezbędnych do oceny ryzyka. W erze cyfrowej tajemnica zawodowa stała się atrakcyjnym wektorem ataku nie dlatego, że prawnicy gorzej chronią dane, lecz dlatego, że wokół ich komunikacji zbudowany jest wysoki poziom zaufania możliwy do wykorzystania przeciwko ofierze. Artykuł pokazuje, że decyzje konfiguracyjne (jak ustawienie DMARC w trybie obserwacyjnym) przestają być neutralne prawnie, gdy ryzyko jest przewidywalne. Rozwój generatywnej sztucznej inteligencji dodatkowo potęguje zagrożenia, czyniąc phishing precyzyjnym i masowym jednocześnie.

Autorka analizuje problem w kontekście RODO, prawa brytyjskiego i amerykańskiego, pokazując wspólny mianownik: prawnik podlega rozliczeniu administracyjnemu, dyscyplinarnemu, cywilnemu i reputacyjnemu, podczas gdy dostawcy IT odpowiadają kontraktowo, często z limitami nieproporcjonalnymi do szkód.

Słowa kluczowe: tajemnica zawodowa prawnika, cyberbezpieczeństwo, spoofing, DMARC, RODO, odpowiedzialność administratora danych, Business Email Compromise, sztuczna inteligencja, phishing, ochrona danych osobowych.

Abstract

Confidentiality as an Attack Vector: Reflections on the Structural Gap Between Lawyer Liability and Technological Control. This article analyzes the fundamental disconnect between concentrated legal liability on lawyers as data controllers and distributed control over technical infrastructure by IT providers. Using a domain spoofing incident as a starting point, it reveals a systemic problem: lawyers are accountable for security breaches yet often lack influence over system configuration, response times, or access to risk assessment information. In the digital era, attorney-client confidentiality has become an attractive attack vector – not because lawyers protect data poorly, but because their communications carry high trust levels exploitable against victims. The article demonstrates that configuration decisions (such as DMARC monitoring mode) cease to be legally neutral when risks are foreseeable. Generative AI amplifies threats, making phishing precise and massive simultaneously. Analyzing GDPR, UK, and US law, the author reveals a common pattern: lawyers face administrative, disciplinary, civil, and reputational accountability, while IT providers have contractual liability often disproportionate to actual damages.

Keywords: attorney-client privilege, cybersecurity, spoofing, DMARC, GDPR, data controller liability, Business Email Compromise, artificial intelligence, phishing, data protection.

Tajemnica zawodowa prawnika nigdy nie była wyłącznie wartością etyczną ani elementem kultury zawodowej. Stanowiła i stanowi konstrukcję prawną, obciążoną odpowiedzialnością osobistą. W erze cyfrowej doszedł do niej jeszcze jeden wymiar, który długo pozostawał niedostrzegany lub bagatelizowany: tajemnica zawodowa stała się atrakcyjnym wektorem ataku. Nie dlatego, że prawnicy gorzej chronią dane, lecz dlatego, że wokół ich komunikacji zbudowany jest wysoki poziom zaufania.

A zaufanie w cyberprzestrzeni jest walutą, którą można ukraść i użyć przeciwko ofierze.

Ten tekst nie jest opowieścią o incydencie IT ani o problemach z administracją systemów. Jest próbą opisanego systemowego błędu, w którym odpowiedzialność prawna i zawodowa została skoncentrowana na prawniku i kancelarii jako administratorze danych, podczas gdy realna kontrola nad infrastrukturą techniczną pozostaje rozproszona pomiędzy dostawców usług, administratorów, operatorów poczty, systemów nazw domen (DNS), hostingu oraz zewnętrzne procedury obsługi zgłoszeń. W tym modelu prawnik odpowiada za skutki, ale nie zawsze ma wpływ na konfigurację, tempo reakcji ani dostęp do informacji niezbędnych do oceny ryzyka. Ten rozdzźwięk był problematyczny już przed erą generatywnej sztucznej inteligencji. Dziś staje się zagrożeniem systemowym.

Punktem wyjścia jest incydent polegający na podszyciu się pod domenę (spoofing). Zaczyna się banalnie: automatyczna wiadomość z systemu obsługi poczty informuje o niedostarczeniu e-maila zatytułowanego „You have been selected!”. Nadawcą ma być adres prawnika prowadzącego kancelarię. Prawnik wie, że tej wiadomości nie wysłał. W tym miejscu kończy się wspólny język prawnika i IT.

Dla zespołu technicznego jest to „odbity e-mail” (bounced mail), zdarzenie operacyjne, które nie doszło do skutku i wymaga sprawdzenia dzienników systemowych.

Dla prawnika jest to sygnał zupełnie innej kategorii: potencjalne naruszenie integralności komunikacji objętej tajemnicą zawodową oraz ryzyko, że jego tożsamość zawodowa jest używana jako narzędzie ataku na klientów.

Ta różnica w percepcji nie wynika z nadwrażliwości ani braku zaufania do technologii. Jest konsekwencją funkcjonowania prawa i technologii w odmiennych reżimach odpowiedzialności. W polskim i szerzej kontynentalnym modelu prawnym tajemnica zawodowa nie jest postulatem ani „dobrą praktyką”. Jest obowiązkiem ustawowym, wzmocnionym odpowiedzialnością dyscyplinarną i cywilną. Zasady etyki zawodowej idą jeszcze dalej, wprost wiążąc korzystanie z narzędzi elektronicznych z obowiązkiem stosowania zabezpieczeń i szczególnej ostrożności. To nie są miękkie rekomendacje. To normy, których naruszenie ma realne konsekwencje.

Dlatego prawnik nie pyta w pierwszym odruchu, czy doszło do awarii. Pyta, czy ktoś podszywa się pod jego domenę i wykorzystuje ją jako maskę do ataku na osoby, które mają prawo ufać, że komunikują się z pełnomocnikiem.

W opisywanym przypadku, analiza nagłówków wiadomości prowadziła do infrastruktury poza Unią Europejską, do adresu IP zarejestrowanego w Stanach Zjednoczonych. Sam fakt transgraniczności nie jest jeszcze rozstrzygający, bo globalna poczta elektroniczna z natury jest rozproszona. Kluczowe było coś innego. Domena kancelarii miała wdrożone mechanizmy

uwierzytelniania nadawcy (SPF i DKIM)¹, ale polityka weryfikacji domeny (DMARC – Domain-based Message Authentication, Reporting and Conformance)², czyli domenowa polityka uwierzytelniania, raportowania i zgodności była ustawiona na tryb obserwacyjny (p=none). W języku technicznym oznacza to monitorowanie. W języku prawnym oznacza to brak realnej bariery przed podszywaniem się.

Protokół SMTP historycznie nie weryfikuje pola „From”. Podszywanie się pod cudzą domenę nie wymaga włamania ani dostępu do systemów ofiary. Wystarczy wysłać wiadomość z odpowiednio ustawionym nagłówkiem. Mechanizmy SPF i DKIM redukują ryzyko, ale dopiero polityka DMARC w trybie kwarantanny lub odrzucenia (p=quarantine albo p=reject) daje serwerom odbiorczym jednoznaczną instrukcję reakcji. Ustawienie p=none mówi wprost: zauważ problem, ale go nie blokuj. Dla wielu dostawców IT jest to „etap wdrożenia”. Dla atakującego jest to zaproszenie. Dla prawnika jest to strefa ryzyka, za którą odpowiada osobiście.

W Unii Europejskiej ten ciężar odpowiedzialności jest opisany precyzyjnie w Rozporządzeniu o Ochronie Danych Osobowych (RODO). Ochrona danych nie polega na „staraniach”, lecz na wdrożeniu odpowiednich środków technicznych i organizacyjnych oraz na zdolności wykazania ich adekwatności. Zasada integralności i poufności, ochrona danych w fazie projektowania (privacy by design), obowiązek reagowania na incydenty w ciągu 72 godzin oraz wymóg stosowania środków odpowiednich do ryzyka tworzą reżim, w którym techniczna neutralność konfiguracji przestaje być neutralna prawnie. Jeżeli spoofing jest ryzykiem przewidywalnym, powszechnie opisanym, a DMARC w trybie odrzucenia jest standardem rekomendowanym w publicznych wytycznych bezpieczeństwa, to utrzymywanie trybu p=none może zostać ocenione jako zaniechanie organizacyjne. Administrator danych nie może bronić się stwierdzeniem, że „to po stronie dostawcy IT”.

W reakcji na incydent prawnik zrobił coś, co bywa interpretowane jako „ominięcie IT”, a w rzeczywistości było racjonalnym działaniem w reżimie osobistej odpowiedzialności. Wydał polecenie natychmiastowej zmiany polityki DMARC na tryb odrzucenia, zabezpieczył ścieżkę dowodową, zażądał dzienników systemowych pozwalających wykazać, że wiadomość nie wyszła z infrastruktury kancelarii, i sam zgłosił zdarzenie do zespołu reagowania na incydenty (CERT – Computer Emergency Response Team, zespół reagowania na incydenty komputerowe). Po jednej stronie padło zdanie: „CERT zrobiony. Potrzebuję logów, żeby wykazać, że to nie wyszło od nas”. Po drugiej: „Temat konfiguracji SPF/DKIM/DMARC przekazany do naszych administratorów”.

To zestawienie jest miniaturą systemu. Dla IT jest to procedura, zgłoszenie, umowa o gwarantowanym poziomie usług (SLA – Service Level Agreement, umowa o poziomie świadczenia usług). Dla prawnika oznacza to okno ryzyka, w którym domena kancelarii nadal może być wykorzystywana jako narzędzie ataku na klientów. Ryzyko to może mieć konkretny wymiar prawny, reputacyjny i ostatecznie – osobisty.

Prawo nie zna pojęcia „czasu reakcji opisanego w umowie o poziomie świadczenia usług (SLA)”. Zna natomiast pojęcie ryzyka i obowiązku jego minimalizacji. Europejskie przepisy

¹ SPF (Sender Policy Framework) i DKIM (DomainKeys Identified Mail) to mechanizmy uwierzytelniania e-maili: SPF potwierdza uprawnienie nadawcy do wysyłania wiadomości z danej domeny, a DKIM zapewnia integralność treści poprzez podpis kryptograficzny, ograniczając phishing i spoofing.

² DMARC to mechanizm, który łączy SPF i DKIM oraz pozwala odrzucać nieautoryzowane e-maile, ograniczając phishing i spoofing.

o ochronie danych osobowych nie operują kategorią „nieudanej próby ataku”. Operują kategorią ryzyka dla praw i wolności osób. Jeżeli ktoś może wiarygodnie podszyć się pod administratora danych, ryzyko już istnieje, niezależnie od tego, czy doszło do wycieku. Administrator danych musi być w stanie wykazać, jakie środki ochrony były wdrożone w momencie zdarzenia i dlaczego były adekwatne do znanego i przewidywalnego ryzyka. W tym sensie konfiguracja techniczna przestaje być neutralna prawnie.

W tym miejscu ujawnia się kolejny problem systemowy: umowy SLA. Z perspektywy prawnika nie są one dokumentami technicznymi, lecz instrumentami zarządzania odpowiedzialnością. Tymczasem standardowe SLA koncentrują się na dostępności usług i czasie usunięcia awarii, pomijając fakt, że w przypadku incydentów bezpieczeństwa stawką nie jest komfort użytkownika, lecz integralność komunikacji objętej tajemnicą zawodową.

Jeżeli umowa przewiduje reakcję na incydent w ciągu 24 lub 48 godzin, to z perspektywy prawa oznacza to 24 lub 48 godzin tolerowanego ryzyka³. Jeżeli kancelaria nie ma umownego prawa do natychmiastowego polecenia zmiany krytycznych ustawień bezpieczeństwa, odpowiedzialność pozostaje po jej stronie, nawet jeśli decyzja techniczna formalnie leży gdzie indziej. Jeżeli umowa nie gwarantuje dostępu do dzienników systemowych, to administrator danych traci podstawowe narzędzie dowodowe, bez którego nie jest w stanie wykazać należytej staranności ani prawidłowo ocenić, czy doszło do naruszenia wymagającego zgłoszenia w ciągu 72 godzin.

W praktyce odpowiedzialność jest asymetryczna. Prawnika rozlicza się administracyjnie, dyscyplinarnie, cywilnie i właśnie – (a może przede wszystkim?) – reputacyjnie. Dostawca IT odpowiada kontraktowo, często w granicach wielokrotności wynagrodzenia, niezależnie od skali szkód. To nie jest problem złej woli. To problem architektury systemu.

W Wielkiej Brytanii, pomimo Brexitu, reżim ochrony danych pozostaje zasadniczo zbieżny, ale dochodzi do niego silnie akcentowany wymiar etyki zawodowej. Rada ds. Regulacji Radców Prawnych (Solicitors Regulation Authority)⁴ traktuje poufność jako obowiązek bezwarunkowy, a phishing i cyberprzestępczość jako element stałego krajobrazu ryzyka. Biuro Komisarza ds. Informacji (Information Commissioner's Office) konsekwentnie wymaga konkretnie: jakie środki wdrożono, dlaczego były adekwatne i jak były nadzorowane⁵. Odpowiedzialność ma twarz i nazwisko, a nie adres e-mail działu IT.

W Stanach Zjednoczonych nie istnieje jednolite prawo ochrony danych na poziomie federalnym, ale obowiązek zachowania kompetencji technologicznej i standard „rozsądnych starań” (reasonable efforts), wyrażony w Modelowych Zasadach Postępowania Zawodowego (Model Rules of Professional Conduct)⁶, prowadzi do bardzo podobnych wniosków: prawnik

³ Por. art. 6 ustawy – Prawo o adwokaturze / art. 3 ustawy o radcach prawnych; § 19–21 KEA / art. 11 KERP; art. 471 i 415 k.c.; art. 266 § 1 k.k.; art. 5 ust. 1 lit. f, art. 32, art. 82 RODO; art. 178 pkt 1 k.p.k.

⁴ Zob. https://www.sra.org.uk/solicitors/guidance/confidentiality-client-information/?utm_source=chatgpt.com

⁵ Zob. art. 24 oraz art. 32 rozporządzenia (UE) 2016/679 (RODO) – obowiązek wdrożenia odpowiednich technicznych i organizacyjnych środków bezpieczeństwa oraz wykazania ich adekwatności i skuteczności (zasada rozliczalności), w powiązaniu ze stanowiskiem Information Commissioner's Office, Guide to accountability and governance under the UK GDPR, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/>

⁶ Model Rules of Professional Conduct wymagają od prawnika bezwzględneho zachowania poufności informacji klienta oraz posiadania podstawowej wiedzy o ryzykach technologicznych, w tym cyberzagrożeniach (Rule 1.6 oraz Rule 1.1, Comment [8]).
Zob.: https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/

nie może ignorować ryzyk, które są powszechnie znane i przewidywalne. Opinia Formalna 483 (Formal Opinion 483) Amerykańskiego Stowarzyszenia Prawników (American Bar Association) jasno pokazuje, że przygotowanie, nadzór nad dostawcami i sensowne środki ochrony są elementem obowiązku zawodowego, a nie dodatkiem⁷.

W trzech porządkach prawnych wspólny mianownik jest jeden: prawnika się rozlicza. Administracyjnie, dyscyplinarnie, cywilnie, reputacyjnie. IT zazwyczaj odpowiada kontraktowo, często z ograniczeniami odpowiedzialności nieproporcjonalnymi do szkód, jakie może ponieść kancelaria.

Dlaczego poufność staje się wektorem ataku? Bo spoofing i phishing działają nie tam, gdzie technologia jest najsłabsza, lecz tam, gdzie zaufanie jest najwyższe. Relacja klient – prawnik jest zaprojektowana tak, by obniżać czujność. Klient ma ufać, bo inaczej nie ma komunikacji ani obrony. Wiadomość „od prawnika” jest otwierana szybciej, link klikany chętniej, załącznik pobierany bez weryfikacji. Przejęcie poczty biznesowej (Business Email Compromise) jest jedną z najkosztowniejszych form cyberprzestępczości, a kancelarie są szczególnie atrakcyjnym celem, bo operują na rachunkach powierniczych, transakcjach i pilnych dyspozycjach finansowych.

Generatywna sztuczna inteligencja nie tworzy nowej kategorii przestępstw. Ona zmienia skalę i jakość. Phishing przestaje być toporny. Staje się precyzyjny, spersonalizowany i masowy jednocześnie. Modele językowe potrafią pisać jak prawnik, używać właściwego tonu i terminologii, a nawet naśladować styl konkretnej osoby. Jeśli atakujący zdobędzie fragment autentycznej korespondencji, może wygenerować wiadomość kontynuującą wątek (follow-up) idealnie dopasowaną do kontekstu. W takich warunkach DMARC w trybie p=none nie jest neutralną decyzją techniczną. Jest zaproszeniem do nadużycia.

W tym sensie decyzje konfiguracyjne stają się decyzjami prawnymi, nawet jeśli podejmowane są przez osoby, które nie ponoszą konsekwencji prawnych. Prawnik, który „ignoruje IT”, często nie ignoruje ludzi ani kompetencji. Ignoruje model, w którym jego odpowiedzialność jest absolutna, a kontrola rozproszona i opóźniona. W epoce sztucznej inteligencji ten model nie będzie się psuł rzadziej. Będzie się psuł częściej.

Tajemnica zawodowa zawsze była i jest wartością chronioną. Dziś jest też bronią, którą można obrócić przeciwko tym, którzy są zobowiązani ją chronić. Poufność jako wektor ataku nie jest metaforą, a opisem rzeczywistości, na którą zgłoszenia przekazane do administratorów nie są wystarczającą odpowiedzią. Zwłaszcza gdy odpowiedzialność spoczywa na prawniku, który może wprawdzie wynegocjować odpowiednią umowę z dostawcą IT, ale nawet najlepsza umowa nie znosi fundamentalnego problemu: jeśli ktoś zaniechał wdrożenia przewidywalnych środków ochrony, odpowiedzialność prawna i zawodowa i tak spoczywa na administratorze danych. A pytanie, czy bezpieczny hosting nie powinien być prowadzony wewnętrznie przez wykwalifikowany zespół techniczny kancelarii, pozostaje otwarte – i coraz bardziej naglące.

⁷ Formal Opinion 483 (ABA) podkreśla, że cyberataki i phishing są dziś normalnym ryzykiem praktyki prawniczej; w razie incydentu prawnik ma obowiązek rozsądnie ustalić jego zakres, ocenić ryzyko dla danych klienta i poinformować klienta, jeżeli poufność mogła zostać naruszona.
https://www.americanbar.org/groups/professional_responsibility/publications/ethics_opinions/formal_opinion_483/

Bibliografia

Akty prawne i dokumenty regulacyjne

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz.Urz. UE L 119 z 4.5.2016.
2. Ustawa z dnia 6 lipca 1982 r. o radcach prawnych, t.j. Dz.U. z 2024 r. poz. 1684.
3. Ustawa z dnia 26 maja 1982 r. – Prawo o advokaturze, t.j. Dz.U. z 2024 r. poz. 1649.
4. Zbiór Zasad Etyki Adwokackiej i Godności Zawodu, uchwała Naczelnej Rady Adwokackiej z dnia 10 października 1998 r. (z późn. zm.).
5. Kodeks Etyki Radcy Prawnego, uchwała Krajowego Zjazdu Radców Prawnych z dnia 22 listopada 2014 r. (z późn. zm.).
6. Data Protection Act 2018 (UK), c. 12.
7. UK GDPR (retained EU law version of the General Data Protection Regulation).
8. American Bar Association, Model Rules of Professional Conduct, 2023.

Opinie, wytyczne i stanowiska organów regulacyjnych

1. American Bar Association, Formal Opinion 483: Lawyers' Obligations After an Electronic Data Breach or Cyberattack, 2018.
2. Solicitors Regulation Authority, Warning notice: Email scams and cyber-attacks targeting law firms, 2024, (<https://www.sra.org.uk/solicitors/guidance/ethics-guidance/cyber-attacks>).
3. Information Commissioner's Office, Guide to the UK General Data Protection Regulation (UK GDPR), (<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources>).
4. European Union Agency for Cybersecurity (ENISA), Threat Landscape Report 2024, (<https://www.enisa.europa.eu>).

Standardy techniczne

1. Internet Engineering Task Force (IETF), RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC), March 2015, (<https://tools.ietf.org/html/rfc7489>).
2. Internet Engineering Task Force (IETF), RFC 7208: Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, April 2014.
3. Internet Engineering Task Force (IETF), RFC 6376: DomainKeys Identified Mail (DKIM) Signatures, September 2011.

Literatura przedmiotu

1. European Data Protection Board, Guidelines 01/2021 on Examples regarding Data Breach Notification, Version 2.0, 2022.
2. FBI Internet Crime Complaint Center, 2023 Internet Crime Report, 2024, (<https://www.ic3.gov>).
3. Ponemon Institute, 2024 Cost of a Data Breach Report, IBM Security, 2024.
4. CERT Polska, Raporty i ostrzeżenia dotyczące incydentów bezpieczeństwa, (<https://www.cert.pl>).

Rzecz o narzędziu do „standaryzacji” analizy i czynności sprawozdawania z oględzin zapisów video lub dokumentacji fotograficznej w prowadzonych postępowaniach

Niemal każde postępowanie prowadzone przez funkcjonariuszy związane jest z koniecznością zabezpieczenia dowodów. W zależności od charakteru sprawy i ilości ujawnionych urządzeń gromadzących dane, konieczne jest dokonanie odczytania zapisów z tych urządzeń. Niejednokrotnie konieczne jest sporządzenie dokumentacji fotograficznej miejsca oraz dokonanie odczytu z zapisów monitoringu video. Odczyt danych z urządzeń takich jak komputer, tablet, nawigacja, telefon komórkowy czy dowolny inny nośnik, realizowane jest za pomocą specjalistycznego oprogramowania. Oprogramowanie to pozwala odczytać zapis z nośników tych urządzeń oraz na dokonanie analizy w celu ujawnienia dowodów. W pewnych przypadkach związanych głównie z telefonami jedynym sposobem zabezpieczenia odczytania i zabezpieczenia tego, co zostało na nich zapisane, począwszy od historii połączeń, wiadomości, zdjęć czy notatek, pozostaje akwizycja manualna, oczywiście pod warunkiem, że po uruchomieniu jest dostęp do jego zawartości. Po zabezpieczeniu dowodów konieczne jest dokonanie oględzin, analiza odczytanych i zabezpieczonych zapisów oraz ocena pozyskanego materiału. W przypadku zapisów video, których analiza wymaga przeglądu z zapisów całości lub zapisów pochodzących z określonego okresu niekiedy wybrania zapisów kilku godzin lub minut, które są istotne dla prowadzonego postępowania lub w przypadku przeglądu dokumentacji fotograficznej, przeprowadzenie oględzin wymaga spisania protokołu. Biorąc pod uwagę konieczność oględzin materiałów uzyskanych z zapisów systemów monitoringu lub dokumentacji fotograficznej związanej z akwizycją manualną możemy dojść do wniosku, że czasochłonność procesu oględzin takich materiałów może być bardzo duża, oczywiście, jeśli nie mamy ograniczonych ram czasowych dla zapisów wymagających oględzin. Z całą pewnością funkcjonariusze dokonujący oględzin ww. materiału dowodowego realizują to zgodnie z wymaganiami procedury karnej i przyjętymi uzgodnieniami prowadzenia oględzin oraz jej gromadzenie. Często funkcjonariusze prowadzący czynności oględzin i sprawozdawania narzekali na uciążliwość i czasochłonność tych czynności. Brak umiejętności związanych ze sposobami obróbki posiadanego materiału dowodowego poprzez powiększenie lub wybór wycinka zdjęcia lub dokonanie przycięcia istotnego fragmentu z wielogodzinnego zapisu video, skutkowało obszernym opisem dotyczącym oględzin takiego materiału. W ostatnim czasie pojawiło się wiele aplikacji pozwalających dokonywać oględzin związanych głównie z zapisem z monitoringu. Oprogramowanie bardzo rozbudowane, wyposażone w filtry pozwalające w oparciu o bazę referencyjną obrazów takich jak; rysy twarzy lub postaci, numerów rejestracyjnych pojazdów i ich koloru, pozwala wyodrębnić fragmenty z zapisów video, odpowiadające warunkom zadany do przeszukania i po ich znalezieniu dokonać wyodrębnienia i zapisu do wskazanego wcześniej folderu. Takie aplikacje stanowią duży skok, jeśli chodzi o samą analizę posiadanych zapisów video, niekiedy również zdjęć. Z uzyskanych w ten sposób materiałów pozostaje napisanie protokołu oględzin materiału dowodowego. Powstające oprogramowanie do analizy zapisów video i zdjęć najczęściej pisane jest jako aplikacja do systemu autorskiego zgodnie

z potrzebami zamawiającego a funkcjonalność, pozwalająca na sporządzenie protokołu z oględzin dla podmiotów jest zbędna. Spośród różnych programów wspierających pracę funkcjonariuszy związanych z analizą nagrań video oraz materiału fotograficznego, jest program Forevid. Program ten przeznaczony jest do analizy i tworzenia raportów z analizy filmów stanowiących dowód w postępowaniach, pozyskanych z monitoringu lub elektronicznych nośników rejestrujących materiały w formie filmów wideo lub zdjęć. Program ten napisany został przez Antti Lehmussola z Narodowego Biura Śledczego w Finlandii, pozyskany i przetłumaczony na język polski dla celów Służby Celnej przez Krajową Grupę Zadaniową ds. Kontroli Gier Hazardowych. Oprogramowanie Forevid Video Analyzer w wersji 1.2.1 dostępne jest pod adresem: <https://forevid.com> w wersji anglojęzycznej. Przetłumaczona na język polski wersja ma nr 1.2.2 na Powszechnej Licencji Publicznej GNU (GPLv2), jest do pobrania pod adresem: <https://drive.google.com/file/d/19-OZJZhLpXC9VXQVbF6H2cLCCr6Y49ID/view?usp=sharing>



Forevid jest programem typu open source służącym do kryminalistycznej analizy nagrań z monitoringu. Forevid oferuje szeroki zestaw funkcji wymaganych w pracy nad sprawą kryminalistyczną, w tym np. różne opcje odtwarzania wideo, przetwarzania i dokumentacji wyników. Forevid używa dobrze znanego serwera Avisynth¹ jako zaplecza do przetwarzania wideo. Aplikacja wyposażona jest w funkcjonalność przydatną podczas prac związanych z analizą kryminalną i posiada:

- ✓ Zarządzanie projektem. Każdy przypadek jest traktowany jako osobny projekt, który pomaga (i zmusza) do organizacji pracy.
- ✓ Rozbudowaną obsługę formatów wideo i kodeków. Oprogramowanie zawiera wbudowaną obsługę dużej liczby różnych formatów wideo i kodeków. Co więcej, wsparcie można rozszerzyć za pośrednictwem Framework Microsoft DirectShow. Jeśli niektóre filmy można odtwarzać tylko za pomocą zastrzeżonych odtwarzaczy, takie filmy można zaimportować za pomocą nagrywania ekranu.
- ✓ Filtry przetwarzania wideo. Dzięki różnym filtrom do przetwarzania wideo można wykonywać operacje, takie jak blokowanie usuwania artefaktów, usuwanie przeplotu, poprawianie histogramu, usuwanie szumów, zmiana rozmiaru, wyostrażanie itp.
- ✓ Wiele opcji eksportu. Z oprogramowania można eksportować zdjęcia w różnych formatach, a także ponownie zakodowane filmy. Co więcej, za pomocą edytora obrazów nieruchomych do obrazów można dodawać strzałki, kształty, tekst itp., a także stosować efekty, takie jak rozmycie, pikselizacja² lub reflektory.

¹ AviSynth (w skrócie AVS) jest potężnym narzędziem przeznaczonym do obróbki wideo. Działa jako serwer klatek, zapewniając możliwość natychmiastowej edycji bez potrzeby tworzenia plików tymczasowych.

² Pikselizacja to zjawisko deformacji obrazu, polegające na widocznym wyświetlaniu poszczególnych pikseli, co sprawia, że obraz staje się mniej płynny i bardziej "pikselowy". Proces ten może być wykorzystywany w celach artystycznych lub technicznych, na przykład w grach komputerowych i animacjach. Pikselizacja może wystąpić przypadkowo, gdy obraz jest powiększany zbyt mocno przy danej rozdzielczości lub celowo, aby uzyskać ciekawe efekty wizualne.

- ✓ Dokumentację wyników analizy. Najciekawsze klatki filmów z przypadkami można dodawać do zakładek i dodawać adnotacje, aby lepiej zrozumieć interesujące wydarzenia.
- ✓ Różne inne opcje, takie jak interfejs skryptowy, edycja wideo, przeglądanie metadanych, obliczanie skrótów itp.

Wymagania programowe/sprzętowe dla Forevid:

- ✓ system operacyjny Windows (XP, Vista lub wyższy);
- ✓ karta graficzna kompatybilna z OpenGL;
- ✓ brak minimalnego limitu pamięci lub miejsca na dysku twardym, im więcej tym lepiej.

Instalacja aplikacji Forevid

Najpierw pobierz program instalacyjny Forevid-1.2.2 exe i uruchom go. Program instalacyjny poprosi Cię o podanie lokalizacji instalacji, aby mógł skopiować niezbędne pliki do podanego folderu. **Jeśli nie masz niezbędnych uprawnień do kopiowania plików do danego folderu, instalacja zakończy się niepowodzeniem.** Dodatkowo instalator wygeneruje folder projektu Forevid. Gdy proces instalacji przebiegnie prawidłowo na pulpicie pojawi się ikona skrótu do programu.

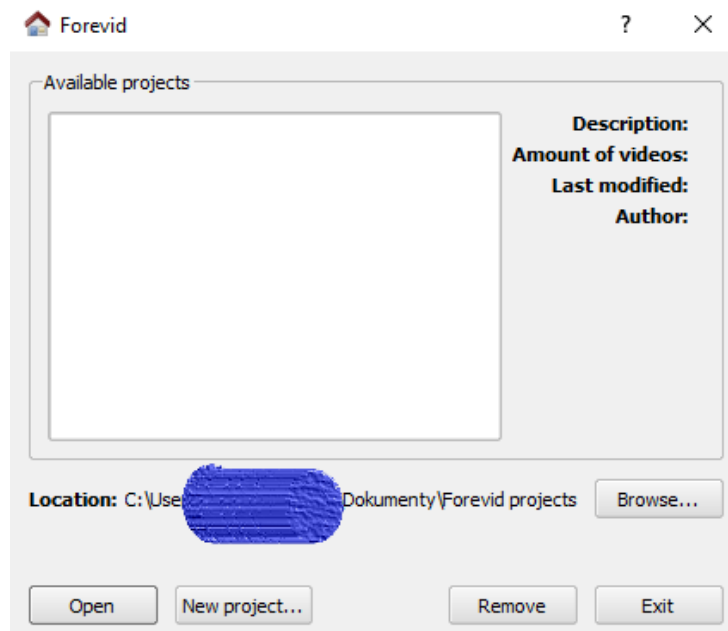


Aby uruchomić Forevid, kliknij dwukrotnie ikonę.

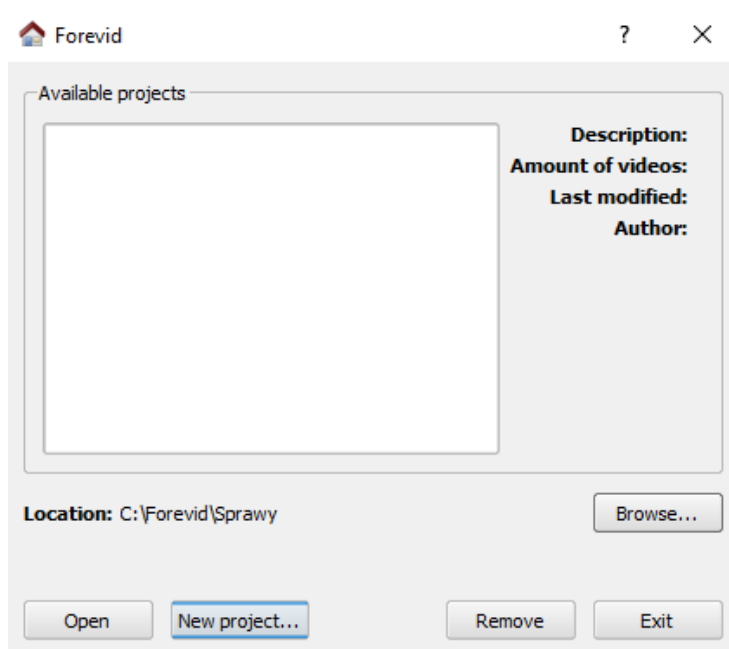
Należy zauważyć, że po zainstalowaniu programu Forevid w wersji 1.2.2 dostępna jest instrukcja obsługi programu w języku polskim i umieszczona w pliku **manual.html**, który znajduje się w folderze: **C:\.....\Forevid\doc**. W tym samym folderze umieszczona jest również skrócona wersja obsługi tego programu umieszczona w pliku **quick.html**, zawierająca opis funkcji przypisanych określonym ikonom występującym w aplikacji.

Pierwsze uruchomienie programu Forevid

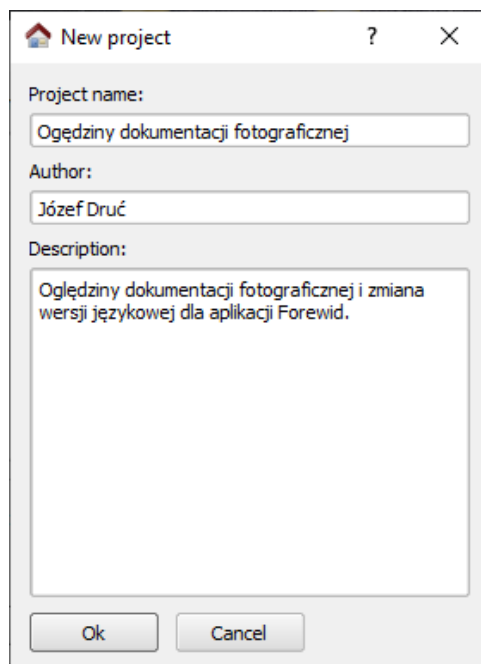
Jeśli proces instalacji przebiegł prawidłowo, a na pulpicie zgodnie z opisem pojawiła się ikona skrótu do programu to po dwukrotnym kliknięciu uruchomi się aplikacja. Pierwsze uruchomienie aplikacji nastąpi w angielskiej wersji językowej z domyślnie ustawionymi ścieżkami lokalizacji plików związanych z prowadzeniem spraw. Jeśli lokalizacja instalacji programu nie jest w jakiś sposób krytyczna można pozostawić ścieżki przyjęte domyślnie.



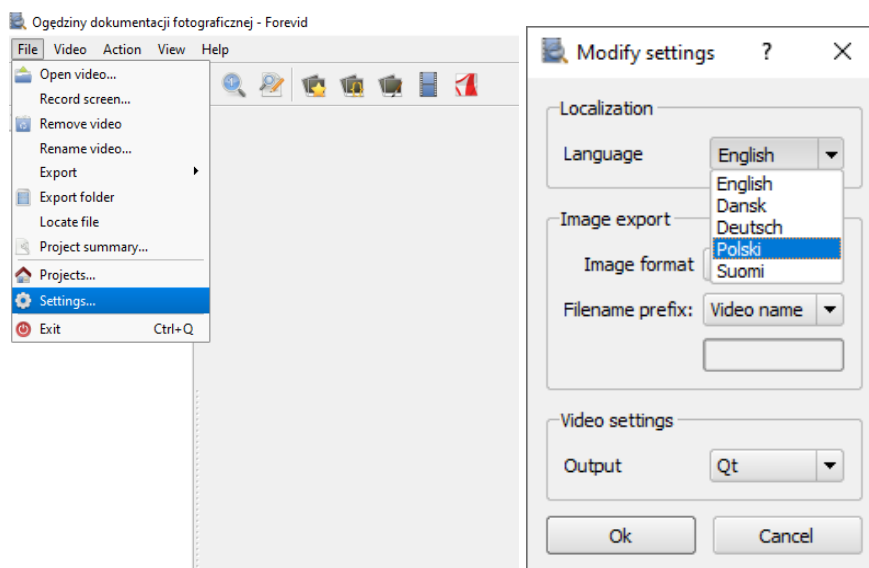
Jeśli ktoś zarządza swoimi zasobami w inny sposób możliwe jest dokonanie zmiany lokalizacji folderu, w którym zapisywane będą pliki dla prowadzonych operacji i oględzin plików. W tym celu należy kliknąć w przycisk **Browse...** i dokonać wyboru ustawienia wymaganego folderu.



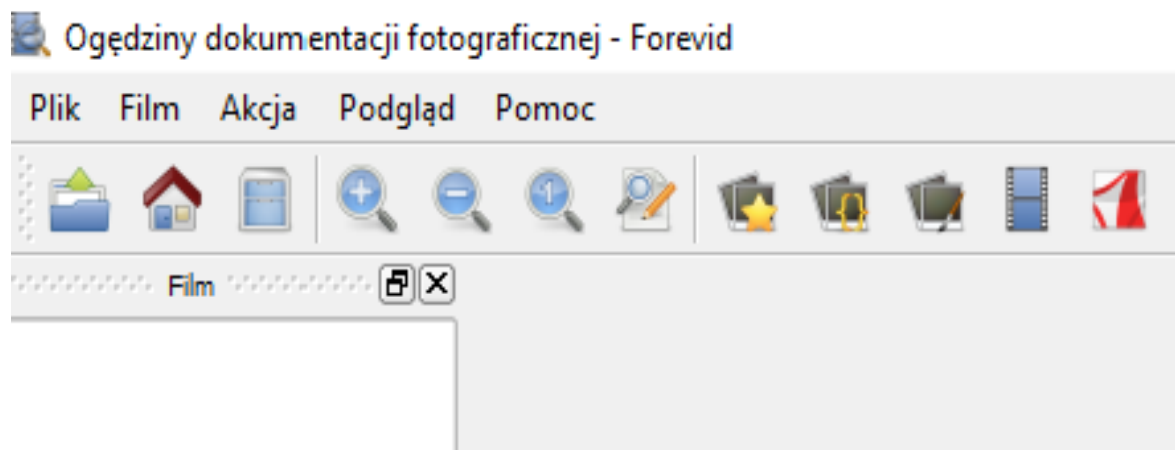
Przy pierwszym uruchomieniu podczas zakładania pierwszej sprawy do analizy można dokonać zmiany wersji języka aplikacji na język polski. Aby tego dokonać musimy kliknąć na buton **New project...**



Po wpisaniu nazwy projektu, danych autora oraz opisu sprawy należy zatwierdzić wpisane dane poprzez kliknięcie na button **OK**. Aplikacja uruchomi się z pulpitem w języku angielskim, ale z tytułem projektu, którego nazwę wpisaliśmy wypełniając okno **Project name**. Następnie dokonując wyboru w menu rozwinieamy kolumnę opisaną jako **File**, po czym z rozwiniętego menu wybieramy opcję **Settings...** co spowoduje wyświetlenie okna do wyboru opcji modyfikacji ustawień. Po rozwinięciu listy **Language** wybieramy z dostępnych opcji **Polski** wybór zatwierdzając buttonem **OK**.



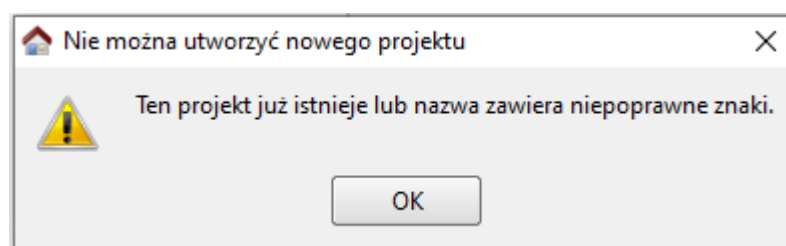
Aby ustawienia wersji językowej zadziałały konieczne jest ponowne uruchomienie aplikacji.



Tak skonfigurowana aplikacja gotowa jest do pracy dla użytkownika posługującego się językiem polskim.

Rozpoczynanie nowego projektu

Nowy projekt jest tworzony w oknie zarządzania projektem. Przy każdym nowym projekcie podawana jest nazwa projektu, opis i autor. Później te informacje będą wyświetlane dla wszystkich Twoich projektów w oknie zarządzania projektami. Projekty tworzą strukturę folderów, której folder główny jest wyświetlany w polu Lokalizacja. Z tego powodu nazwa projektu może zawierać tylko znaki dozwolone w nazwach folderów systemu Windows. Lokalizację folderu głównego projektu można zmienić, naciskając przycisk Przeglądaj.... Po utworzeniu nowego projektu lub otwarciu starego projektu otwierane jest główne okno programu Forevid. W przypadku wpisania projektu o tej samej treści, która jest już wpisana pojawi się komunikat:



Uzyskiwanie dostępu do starych projektów

W oknie zarządzania projektami wyświetlana jest lista wszystkich projektów znajdujących się w folderze głównym projektu. Dodatkowo wyświetlany jest opis projektu, ilość filmów, czas ostatniej modyfikacji i autor dla każdego projektu. Istniejący projekt można otworzyć, wybierając nazwę projektu i naciskając przycisk Otwórz. Podobnie, istniejący projekt można usunąć, naciskając przycisk Usuń. Gdy projekt zostanie usunięty, folder projektu i cała jego zawartość zostaną trwale usunięte.

Interfejs użytkownika

Po utworzeniu nowego projektu lub otwarciu istniejącego projektu wyświetlane jest główne okno programu Forevid. Części interfejsu użytkownika są następujące: wszystkie zaimportowane filmy są wymienione po lewej stronie, wszystkie zakładki są wymienione po

prawej stronie, a wyświetlanie wideo i elementy sterujące pośrodku. Na końcu pasek menu zawiera typowe menu, a pasek narzędzi zapewnia dostęp do często używanych poleceń.

Na grafice poniżej przedstawiono główny interfejs użytkownika Forevid: (A) zaimportowane filmy lub zdjęcia, (B) menu i pasek narzędzi, (C) zakładki, (D) elementy sterujące wideo.



Odtwarzanie

Forevid zapewnia odtwarzanie filmów przechowywanych z wieloma różnymi kontenerami i kodekami. Podczas importowania nowego filmu (przycisk **Plik** → **Otwórz wideo** lub pasek narzędzi) użytkownik może wybrać jedną z następujących metod importowania:

- **FFmpeg** – Wideo jest importowane za pomocą wbudowanej biblioteki FFmpeg. Biblioteka FFmpeg obsługuje szeroką gamę różnych formatów kontenerów i kodeków.
- **DirectShow** – Wideo jest importowane przy użyciu platformy Microsoft DirectShow. Aby pomyślnie zaimportować wideo, system operacyjny musi mieć zainstalowane niezbędne rozdzielacze i kodeki DirectShow.
- **Video for Windows** – Wideo przechowywane w formacie AVI jest importowane przy użyciu starszej struktury Video for Windows firmy Microsoft. Aby pomyślnie zaimportować wideo, plik musi być w formacie AVI, a system operacyjny musi mieć zainstalowany niezbędny kodek VfW.
- **Avisynth script** – Plik skryptu AviSynth jest importowany jako wideo.

Filmy można importować, przeciągając pliki wideo bezpośrednio z Eksploratora Windows na listę zaimportowanych filmów. W takim przypadku wideo jest importowane za pomocą metody FFmpeg. Wszystkie zaimportowane filmy są wyświetlane jako ikony w części Wideo. Domyślnie nazwy importowanych filmów są definiowane przez odpowiadające im nazwy plików, ale można je zmodyfikować, wybierając opcję **Plik** → **Zmień nazwę wideo...** Zmiana nazwy pliku nie powoduje zmiany rzeczywistej nazwy pliku. Jeśli rzeczywisty plik wideo

będzie wymagał późniejszego dostępu, polecenie **File** → **Locate** otworzy folder, w którym znajduje się plik, za pomocą Eksploratora Windows.

Uwaga!

Jeśli z jakiegoś powodu Forevid nie jest w stanie zaimportować danego wideo, zostanie wyświetlone okno dialogowe błędu. Wybierając opcję Media info w oknie dialogowym, można uzyskać szczegółowe informacje o pliku wideo i np. zidentyfikować kod FourCC wymaganego kodeka.

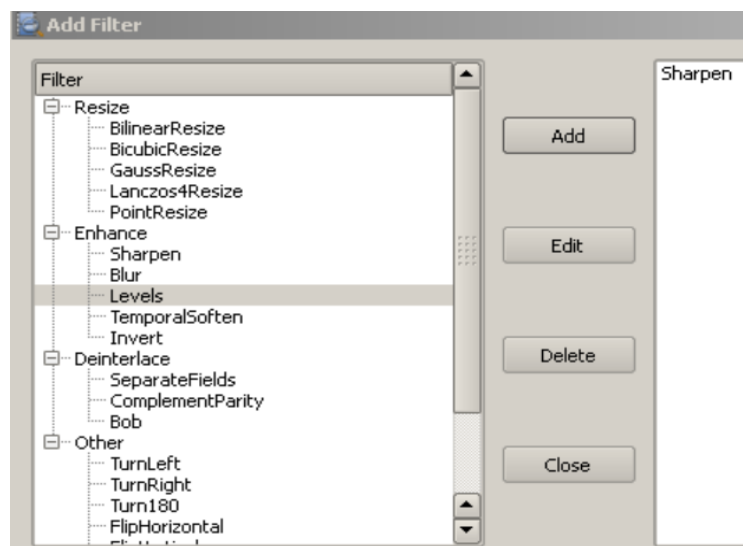
Czasami nagrania z monitoringu są (niestety) przechowywane w zastrzeżonych formatach, które można odtwarzać tylko za pomocą zastrzeżonych odtwarzaczy dostarczonych przez producentów. W takim przypadku wideo może zostać zaimportowane do Forevid za pomocą funkcji nagrywania ekranu, która kopiuje klatki, które są wyświetlane na ekranie podczas odtwarzania wideo za pomocą zastrzeżonego odtwarzacza. Następnie generowany jest nowy nieskompresowany plik wideo i importowany do Forevid.

Przetwarzanie wideo

Do zaimportowanych filmów można zastosować różne operacje przetwarzania wideo. Całe przetwarzanie odbywa się w pamięci komputera, pozostawiając oryginalny film nietknięty. Zastosowane operacje przetwarzania wideo generują łańcuch przetwarzania, który można później modyfikować.

Forevid wyposażono w filtry które są podzielone na cztery kategorie:

- ✓ zmiana rozmiaru,
- ✓ ulepszanie,
- ✓ usuwanie przeplotu,
- ✓ inne.



Wyjaśnienie każdego z wymienionych filtrów oraz sposób działania opisane zostały szczegółowo w instrukcji, do programu, która dostępna jest w języku polskim bezpośrednio po zainstalowaniu aplikacji Forevid w folderze **C:/Forevid/doc/manual.html**.

Przetwarzanie zdjęć uzyskanych podczas analizowania zapisów video

Zdjęcia można generować na różne sposoby. Po pierwsze, najprostszym sposobem na zapisanie interesującej klatki jest naciśnięcie przycisku nagrywania (elementy sterujące wideo są częścią głównego okna). Jest to operacja skrótu, która automatycznie zapisuje nieruchomy obraz w folderze eksportu w predefiniowanym formacie. Konwencję nazewnictwa i format obrazu dla tej opcji można zmodyfikować, wybierając opcję **Plik → Ustawienia**. Po drugie, bieżącą klatkę można wyeksportować do schowka, wybierając **Plik → Eksportuj → Bieżąca klatka do schowka**. Wszystkie zakładki można przechowywać jako nieruchome obrazy, wybierając opcję **Plik → Eksportuj → Klatki** oznaczone zakładkami jako obrazy. Na koniec zestaw kolejnych klatek można zapisać, zaznaczając część osi czasu wideo i wybierając **Plik → Eksportuj → Wybrane klatki jako obrazy**.

Zmodyfikowane filmy wideo można eksportować jako ponownie zakodowane filmy za pomocą **Plik → Eksportuj → Zakodowane wideo**. Kodowanie odbywa się za pomocą kodera x264, który jest najnowocześniejszym koderem do kompresji H.264/MPEG-4 AVC. Parametry kodowania definiuje się poprzez wybranie z listy jednego ze wstępnie zdefiniowanych profili ustawień. Dostępne kontenery dla zakodowanych filmów to Matroska (mkv), MPEG-4 Part 14 (mp4) i Flash (flv). Ponadto zakodowane wideo można wyeksportować w postaci samorozpakowujący się odtwarzacz wideo (SFX Player), który automatycznie odtwarza dołączone wideo.

Edycja zdjęć

Przed zapisaniem wybranej klatki jako obrazu można ją edytować. Odbywa się to poprzez wybranie opcji **Plik → Eksportuj → Bieżąca klatka do edycji**. Następnie bieżąca klatka jest otwierana w edytorze obrazów, jak pokazano na ilustracji poniżej. Wynikowy obraz można zapisać jako obraz lub skopiować do schowka.



Poniżej opisano główne funkcjonalności zaprezentowanego edytora obrazów wchodzącego w skład aplikacji Forevid:

- Powiększ obraz. Powiększa obraz w celach wizualizacji. Nie zmienia rozmiaru obrazu wynikowego.

- Skalowanie obrazu. Skaluje obraz o określoną wartość. Skalowanie można wykonywać dowolnie zarówno w kierunku poziomym, jak i pionowym lub zachowując określone proporcje.
- Modyfikowanie płótna. Zmienia rozmiar i kolor płótna obrazu znajdującego się pod spodem. Ta operacja może służyć do dodawania obramowań wokół oryginalnego obrazu.
- Przytnij obraz. Przycina obraz do określonego rozmiaru. Obszar kadrowania jest wybierany poprzez zmianę rozmiaru podświetlonego obszaru na obrazie.
- Dodawanie wypełnionych kształtów. Dodaje do obrazu obiekty prostokątne, kwadratowe, eliptyczne lub okrągłe. Oprócz kształtu, koloru i krycia obiektów można kontrolować.
- Dodaj kształty z obramowaniami. Podobna do poprzedniej operacji, z tą różnicą, że obiekty zawierają tylko obramowania. Ponadto można wybrać szerokość i styl obramowania.
- Dodaj linie lub strzałki. Dodaje do obrazu linie z grotem strzałki lub bez niego. Można wybrać kolor, szerokość i styl linii.
- Dodaj tekst. Dodaje do obrazu tekst o podanej czcionce, rozmiarze czcionki, kolorze czcionki i kryciu.
- Rozmycie części obrazu. Rozmywa prostokątną, kwadratową, eliptyczną lub okrągłą część obrazu. Stopień rozmycia można kontrolować.
- Pikselizacja części obrazu. Podobnie jak w poprzedniej operacji, z tą różnicą, że zamiast rozmycia, rozdzielczość pod wybranym obszarem jest zmniejszana.
- Wyróżnij część obrazu. Podobne do operacji rozmycia lub pikselizacji, z tą różnicą, że zmienia się jasność lub kontrast zaznaczonego obszaru.
- Dodaj znak wodny. Dodaje dany znak wodny do obrazu. Znak wodny jest podawany jako plik obrazu, a krycie obrazu jest modyfikowane.

Dokumentacja

Dokumentacja wyników analiz jest istotną częścią każdej sprawy. W programie Forevid możesz dokumentować swoje wyniki, eksportując zdjęcia i ponownie zakodowane filmy lub generując zakładki i raporty PDF. Każdy projekt ma swój własny folder eksportu, w którym domyślnie przechowywany jest cały materiał. Dostęp do folderu eksportu można uzyskać, wybierając opcję **Plik → Eksportuj folder** (lub za pomocą odpowiedniego przycisku na pasku narzędzi).

Zakładki

Lokalizacja najciekawszych ramek może być przechowywana wraz z zakładkami. Zakładka jest tworzona przez wybranie opcji **Akcja → Dodaj zakładkę** (lub za pomocą przycisku paska narzędzi). Spowoduje to utworzenie zakładki wskazującej lokalizację bieżącej ramki. Dodatkowo można dodać pisemny opis ramy. Wszystkie zakładki są wyświetlane na liście zakładek. Po kliknięciu zakładki wyświetlana jest ramka oznaczona zakładką. Zakładki i ich opisy można zapisać jako raport PDF, wybierając opcję **Plik → Eksportuj → Zakładki jako PDF**. Przed wygenerowaniem pliku PDF można zmodyfikować szczegóły raportu i lokalizację pliku. Ponieważ istnieje możliwość niedokładnych zakładek, zaleca się wcześniejsze przetestowanie dokładności zakładek tworzenie pliku PDF zatytułowany „Protokół oględzin dokumentacji fotograficznej”.

Dla przykładu wykonano analizę kilku zdjęć dokonując opisu i edycji na obrazie. Wygenerowano też załączony protokół z oględzin analizy zdjęć dla zobrazowania wyników uzyskanych dzięki aplikacji Forevid na przykładzie oględzin i analizy zdjęć zatytułowany „Protokół oględzin dokumentacji fotograficznej”.

Oględziny dokumentacji fotograficznej

Autor: Józef Druć

Opis: Opis: Protokół oględzin dokumentacji fotograficznej. Analizę i raport wygenerowano w celach poglądowych.



Obraz 1. Tablica rejestracyjna pojazdu. (#0, Tablica_1.bmp)



Obraz 2. Pojazd Toyota w ruchu z nadmierną prędkością. (#0, Pojazd w ruchu.bmp)



Obraz 3. Kierowca palący w czasie jazdy e-papierosa. (#0, kierowca palący papierosa.bmp)



Obraz 4. Miejsce spotkań kierowców w bezpośrednim sąsiedztwie obszaru chronionej przyrody Zespołu Przyrodniczo-Krajobrazowego PORZECZE. (#0, Porzecze.bmp)



Obraz 5. Starzy znajomi.Policjant Nosól z posterunku w Sandomierzu.
(#0, Mietek_2.bmp)

Baśnie i legendy o Dysku i Fleszce

„Specjalistą nie jest ten, kto umie coś zrobić, ale ten, kto rozumie, jak to działa”

Okzo

Streszczenie

W publikacji zostały przedstawione problemy techniczne i fizyczne ograniczenia związane z odzyskiwaniem danych. Zostały opisane podstawy działania nośników danych różnych typów, a także występujące w nich usterki z uwzględnieniem ich najbardziej charakterystycznych objawów wyznaczających kierunek diagnostyki. Dla każdej kategorii usterek zostały wskazane zarówno istniejące sposoby ich usuwania oraz techniki odzyskiwania danych, jak też kierunki i stan badań mających na celu opracowanie nowych metod. W końcowej części został przedstawiony proces odzyskiwania danych i zabezpieczenia materiału do dalszej analizy.

Słowa kluczowe: odzyskiwanie danych, cyfrowe nośniki informacji, diagnostyka nośników danych, dysk twardy, SSD.

Abstract

This publication presents the technical challenges and physical limitations associated with data recovery. It describes the basics of operation of various types of data storage media, as well as the faults they can encounter, highlighting their most characteristic symptoms that guide diagnostics. For each fault category, existing methods for their removal and data recovery techniques are identified, along with the directions and status of research aimed at developing new methods. The final section presents the data recovery process and the preservation of the material for further analysis.

Keywords: data recovery, digital storage media, data storage diagnostics, hard drive, SSD.

1. Przedstawienie problemu

Zagadnienie odzyskiwania danych obrosło wieloma mitami i legendami. Kultura popularyzująca często przedstawia bardzo uproszczony obraz pracy funkcjonariuszy Policji i innych służb. W świecie fikcji dysponują oni różnorodnymi magicznymi walizeczkami i pudełeczkami pozwalającymi na odzyskiwanie danych oraz przełamywanie zabezpieczeń i uzyskiwanie dostępu do znajdujących się na różnych nośnikach informacji w szybki i prosty sposób.

Wiarę w ten fikcyjny świat podsycają także niezbyt fortunne wypowiedzi nietechnicznych urzędników, prokuratorów, komendantów, czy oficerów prasowych. Bez wskazywania konkretnych przykładów, bo nie chodzi tu o krytykę konkretnych wypowiedzi konkretnych osób, jednak osoby zabierające głos i zajmujące stanowisko w imieniu służby powinny mieć świadomość tego, że słowa publicznie rzucone dla dodania sobie animuszu i pewności siebie mogą rodzić nierealistyczne oczekiwania wobec pracy innych funkcjonariuszy, zwłaszcza techników kryminalistyki. Realistycznej oceny możliwości odzyskiwania danych nie ułatwiają także oderwane od technicznej wiedzy przepisy regulujące procedury niszczenia danych [Kaczmarzyk 2024c], nie

zawsze rzetelnie wykorzystywane przez firmy niszczące dane dla sugerowania tajemniczych, nieuzasadnionych prawami fizyki i wiedzą techniczną możliwości laboratoriów różnych służb.

W rzeczywistości funkcjonariusze często przy wykonaniu zadań borykają się z licznymi trudnościami. Nie dysponują ani magicznymi pudełeczkami znanymi z kryminalnych seriali, ani fantastycznymi super mocami. Często przy tym pewne zadania nie są rozwiązywane przez wewnętrzne laboratoria kryminalistyczne, ale organy zlecają ich wykonanie komercyjnym firmom, w tym oferującym podobne usługi na otwartym rynku. Przyczyny takiego stanu rzeczy są złożone i obejmują wiele czynników, od dostępnego wyposażenia i możliwości zakupu niezbędnych części po system szkolenia funkcjonariuszy, w jakim nierzadko najważniejsze jest, by liczba przyniesionych do kadr zaświadczeń się zgadzała.

W praktyce o tym, czy dane są możliwe do odzyskania, czy nie, decydują prawa fizyki. Cyfrowa informacja jest interpretacją pewnych stanów fizycznych reprezentujących logiczne jedynki i zera. Szczegóły fizycznej reprezentacji stanów logicznych oraz procesów kodowania i dekodowania różnią się w zależności od typu nośnika, jednak dopóki odpowiednie stany fizyczne wciąż istnieją, dane są odzyskiwalne, a jeśli zostaną zniszczone lub zmienione, odzyskanie danych staje się niemożliwe.

Niestety nie żyjemy w idealnym świecie i nie w każdym przypadku, kiedy odzyskanie danych teoretycznie jest możliwe, w praktyce faktycznie zostaną one odzyskane. Często na przeszkodzie uzyskaniu pozytywnego rezultatu stają ograniczenia budżetowe, czasowe lub technologiczne. Istotnym problemem okazuje się dostępność dawców, zwłaszcza w przypadku niszowych, mało popularnych modeli dysków.

Zdarza się też, że odzyskiwanie danych kończy się niepowodzeniem, a nawet bezpowrotną utratą danych w wyniku ludzkich błędów [Kaczmarzyk 2025b]. Przy czym odzyskiwanie danych obejmuje bardzo szeroką gamę zadań od tak prostych, że nawet laik posługujący się najbardziej prymitywnymi programami może sobie poradzić, po tak skomplikowane, że kwalifikowałyby się na duże projekty naukowe, gdyby ktokolwiek zapewnił zasoby adekwatne dla ich realizacji. Dlatego też w pewnych sytuacjach nawet najlepsi specjaliści są bezradni, choć dane z fizycznego punktu widzenia są odzyskiwalne. Z drugiej strony zbyt często można spotkać krytyczne błędy wynikające z niekompetencji, pochopnego podejmowania działań nieuzasadnionych diagnostyką (w skrajnych przypadkach wręcz z pominięciem diagnostyki), niedbalstwa oraz lekceważenia podstawowych dobrych praktyk i zasad zabezpieczania nośników.

W dalszych częściach publikacji zostaną przedstawione podstawowe zasady działania nośników danych oraz przyczyny utraty dostępu do informacji. Dla każdej z kategorii usterek zostaną opisane dostępne metody postępowania, a także praktyczne i fizyczne granice możliwości odzyskiwania danych. Zostaną też wskazane kierunki rozwoju technik odzyskiwania danych, jakie w przyszłości mogą doprowadzić do zmniejszenia „szarej strefy” pomiędzy ograniczeniami o charakterze praktycznym i fizycznym. Opis każdej kategorii usterek obejmuje najbardziej typowe objawy pozwalające z dużym prawdopodobieństwem zakwalifikować uszkodzenie do właściwej kategorii. Na koniec zostaną wskazane najważniejsze zasady postępowania i dobre praktyki pozwalające ograniczyć ryzyko pogorszenia stanu zabezpieczanych nośników i utraty możliwości odzyskania danych.

2. Podstawy działania nośników danych

Cyfrowe nośniki danych bardzo istotnie różnią się między sobą w zakresie budowy, rozwiązań konstrukcyjnych, zasad funkcjonowania i fizyki przechowywania informacji. Różnice te przekładają się na podatności na usterki oraz stosowane metody i możliwości odzyskania danych. Tym niemniej możliwe jest przedstawienie ogólnego modelu funkcjonowania nośników danych, analogicznego do modelu ISO/OSI RM opisującego strukturę komunikacji w sieci komputerowej. W pewnym sensie na nośniki danych można też spojrzeć jak na urządzenia służące przekazywaniu informacji, tyle, że nie na odległość, a w czasie.

Interpretacja logiczna	Programy obsługujące różne formaty plików
Adresowanie logiczne	MBR, GPT, systemy plików, RAID
Protokoły komunikacyjne	ATA, SCSI, SD/eMMC, NVMe, USB
Adresowanie fizyczne	LBA<->PBA, FTL, TRIM
Kodowanie/dekodowanie	MFM, RLL, XOR, ECC
Stany logiczne	„0” i „1” – interpretacja zależy od przyjętej konwencji
Stany fizyczne	Namagnesowanie, ładunek elektryczny, odbicie światła, rezystancja

2.1. Interpretacja logiczna

Z punktu widzenia użytkownika dane są przechowywane w postaci plików – zorganizowanych całości zawierających informację określonego typu zapisaną w określonym formacie. Mogą to być dokumenty tekstowe, arkusze kalkulacyjne, obrazy, bazy danych, nagrania audio-wizualne i inne. Każdy typ plików ma określoną wewnętrzną strukturę pozwalającą przedstawiać przy pomocy odpowiedniego oprogramowania jego zawartość w sposób czytelny dla użytkowników.

Zawartość niektórych typów plików może być przynajmniej częściowo odczytywana ze zrozumieniem bezpośrednio w edytorze szesnastkowym (heksadecymalnym) bez użycia dedykowanego oprogramowania. Dotyczy to np. plików tekstowych, czy fragmentów nieszyfrowanych baz danych. Analiza zawartości innych plików bez użycia odpowiednich narzędzi jest praktycznie niemożliwa. W szczególności problematyczne mogą być pliki zaszyfrowane, zabezpieczone hasłami oraz materiały audiowizualne zapisywane z wykorzystaniem nietypowych metod kodowania.

2.2. Adresowanie logiczne

Pliki zwykle są uporządkowane w strukturze katalogów umieszczonej na partycji. Za zarządzanie strukturą logiczną partycji odpowiadają systemy plików. Każda z partycji może być sformatowana w jednym, wybranym przez użytkownika systemie plików, przy tym jeśli na nośniku znajduje się kilka partycji, każda z nich może być sformatowana w innym systemie plików, niezależnie od systemów plików na pozostałych partycjach.

Podział na partycje (z nielicznymi wyjątkami) jest opisywany w tablicach partycji w głównym sektorze rozruchowym (MBR – *Master Boot Record*) lub w tablicach GPT (*GUID Partition Table*). Typowo partycja w całości znajduje się na jednym nośniku, ale możliwe są też

rozwiązania, w jakich znajdzie się ona na kilku dyskach. Najpopularniejszym z tych rozwiązań są macierze RAID (*Redundant Array of Independend Discs*) umożliwiające łączenie wielu dysków w jedną logiczną całość. Ze swego rodzaju wirtualnymi partycjami mamy do czynienia w przypadku plików wirtualnych maszyn zawierających wewnętrzne wirtualne systemy plików. Zresztą podobnie też można spojrzeć i na obrazy binarne wykonywane podczas zabezpieczania dowodów cyfrowych.

Wewnętrzne struktury logiczne systemów plików różnią się między sobą, choć pomiędzy wieloma systemami plików można zauważyć wiele podobieństw i wspólnych założeń ich architektury. Różnice pomiędzy systemami plików oraz preferencje autorów systemów operacyjnych sprawiają, że systemy operacyjne są w stanie obsługiwać tylko wybraną część systemów plików. Dane zapisane w systemie plików nieobsługiwanym przez system operacyjny nie będą pod tym systemem widoczne, gdyż system operacyjny nie będzie w stanie obsłużyć adresowania w strukturze logicznej tego systemu plików.

Nie mamy w tym przypadku do czynienia z faktyczną utratą danych – dostęp do nich z łatwością można uzyskać identyfikując system plików na partycji i montując ją w obsługującym ten system plików systemie operacyjnym. Pewien problem mogą stanowić niszowe systemy plików specyficzne dla konkretnych urządzeń i producentów oraz obsługiwane jedynie przez specyficzne dla tych urządzeń i producentów oprogramowanie. Takie systemy plików można spotkać m. in. w motoryzacji, systemach przemysłowych, urządzeniach Internetu rzeczy, dronach i można się spodziewać, że w miarę postępu technicznego, będą się pojawiały też i w innych urządzeniach, a ich znaczenie będzie rosło [Sheremetov, 2023].

Jest to istotne zagadnienie, z uwagi na to, że urządzenia elektroniczne, różne czujniki i inne podzespoły większych systemów, urządzeń i pojazdów mogą zbierać dane ważne z punktu widzenia informatyki śledczej [Davies 2024, Baraniecki 2025b]. Dane te mogą być tym bardziej istotnymi dowodami cyfrowymi, że ich modyfikacja, możliwości manipulacji nimi, a nieraz nawet sama świadomość ich rejestracji na ogół wymaga od użytkowników wyrażnie większych kompetencji technicznych, niż podobne działania w odniesieniu do danych przechowywanych w komputerach lub smartfonach. Jedną z przyczyn tych trudności jest brak dostępnej dokumentacji, co równocześnie utrudnia analizę zabezpieczanych dowodów.

2.3. Protokoły komunikacyjne

W celu odczytania plików z dysku, trzeba się z nim odpowiednio skomunikować. W początkach techniki komputerowej dominowały zamknięte architektury wykorzystujące wewnętrzne protokoły komunikacyjne producentów. Jednak w miarę rozwoju komputeryzacji pojawiła się potrzeba zapewnienia kompatybilności pomiędzy podzespołami pochodzącymi od różnych producentów. Potrzeba ta doprowadziła do ustandaryzowania protokołów komunikacyjnych.

Pierwszymi standardami opisującymi pracę dysków twardych były opracowane w pierwszej połowie lat '80 standardy SCSI (*Small Computer System Interface*) [<https://www.t10.org/scsi-3.htm>] i ATA (*Advanced Technology Attachment*) [<https://t13.org/index.php/standards-published>]. Z biegiem lat standardy te ewoluowały (np. doczekały się szeregowych implementacji magistrali – *Serial Attached SCSI* i *SATA*) i do tej pory zgodne z nimi są niemalże wszystkie dyski twarde,

większość dysków SSD (*Solid State Drive*) oraz karty pamięci typu *Compact Flash*. Ponadto ze standardu SCSI wywodzi się część innych protokołów komunikacyjnych, m. in. USB (*Universal Serial Bus*) i NVMe (*Non-Volatile Memory Express*).

Ponieważ nośniki danych są urządzeniami blokowymi (w odróżnieniu od urządzeń znakowych, nie pozwalają na adresowanie pojedynczych bajtów – „znaków”, ale adresują dane w większych blokach – stąd ich nazwa), również protokoły komunikacyjne opisują adresowanie i przesyłanie danych w blokach. W czasach, kiedy powstawały standardy SCSI i ATA dyski twarde i niemal wszystkie inne wówczas dostępne nośniki danych adresowały dane w 512-bajtowych sektorach fizycznych, dlatego przyjętą przez te standardy jednostką adresowania danych zostały 512-bajtowe sektory LBA (*Logical Block Addressing*). Wprowadzenie adresacji LBA polegającej na nadawaniu fizycznym sektorom kolejnych numerów od 0 aż do wyczerpania pojemności nośnika było istotnym przełomem.

Wcześniej dane adresowano odwołując się bezpośrednio do fizycznych adresów sektorów w adresacji CHS (*Cylinder-Head-Sector*), co wymagało uwzględnienia różnic w fizycznej adresacji dysków w logicznej adresacji na poziomie systemów plików, czego relikty można spotkać w strukturach logicznych wielu systemów plików. Wprowadzenie adresacji LBA uwolniło systemy plików od konieczności zwracania uwagi na fizyczną adresację, jednocześnie wymuszając na producentach dysków wprowadzenie rozwiązań odpowiedzialnych za przeliczanie adresów LBA na adresy fizyczne. Z drugiej strony, producenci zyskali elastyczność i nowe możliwości w zakresie optymalizacji wykorzystania powierzchni dysków i zarządzania defektami, co w krótkim czasie przyczyniło się do znacznego zwiększenia gęstości zapisu i pojemności dostępnych dysków twardych.

Ponadto ustandaryzowanie protokołów komunikacyjnych oraz wynalezienie adresacji LBA otworzyło drogę do łączenia dysków w macierze RAID [Patterson, Gibson, Katz 1988]. Zbudowanie takich macierzy na wielu dyskach odwołując się bezpośrednio do fizycznej adresacji każdego z nich byłoby niezwykle skomplikowane. Adresacja LBA pozwala, by użytkownik widział dyski jako jedną logiczną całość adresowaną przez ciągłą sekwencję adresów sektorów LBA, jaka jest przeliczana przez kontroler macierzy na adresy LBA poszczególnych dysków.

Wprowadzenie adresacji LBA ułatwiło też wykorzystanie nośników półprzewodnikowych, jak karty pamięci, pendrivy i dyski SSD. Nośniki półprzewodnikowe nie mają talerzy, ścieżek i sektorów, a wewnętrzna adresacja nośnika w układach scalonych typu Flash-NAND jest zupełnie inna, niż w przypadku dysków twardych. Wprawdzie powstały systemy plików opracowane z myślą o nośnikach półprzewodnikowych i uwzględniające ich fizyczną adresację, jak YAFFS i JFFS, jednak z uwagi na dużą różnorodność i tempo zmian zachodzących w układach Flash-NAND oraz ograniczoną liczbę systemów operacyjnych obsługujących te systemy plików, nie zyskały one dużej popularności i można je spotkać tylko w niszowych zastosowaniach.

Niezależna od fizycznej adresacji adresacja LBA pozwala zachować pełną kompatybilność pomiędzy systemami plików oraz nośnikami informacji różnych typów. Przeliczanie przez oprogramowanie układowe wewnętrznych jednostek adresacji o różnych rozmiarach na 512-bajtowe sektory LBA zapewnia tej adresacji dużą odporność na postęp techniczny, co czyni ją uniwersalną i długowieczną. Dlatego jest ona wykorzystywana przez wszystkie powszechnie używane protokoły komunikacyjne służące do obsługi nośników danych.

2.4. Adresacja fizyczna

Adresacja fizyczna w nośnikach danych odnosi się bezpośrednio do fizycznych jednostek alokacji i jest niedostępna dla użytkownika. Nawet, jeśli oprogramowanie diagnostyczne, przeznaczone do odzyskiwania danych lub analizy śledczej posługuje się pojęciem adresów lub sektorów fizycznych, zazwyczaj termin ten odnosi się do adresów LBA. Faktyczne fizyczne adresy odnoszą się do współrzędnych fizycznych sektorów w obrotowym układzie odniesienia na talerzach dysków twardych lub bloków i stron w układach Flash-NAND w nośnikach półprzewodnikowych.

Ponieważ wymiana danych, poleceń i komunikatów pomiędzy nośnikami danych i innymi urządzeniami odbywa się z wykorzystaniem adresacji LBA, konieczne jest przeliczanie adresów LBA na fizyczne. Odpowiada za to część oprogramowania układowego nośnika nazywana translatorem. Z uwagi na istotne różnice w budowie i fizyce przechowywania informacji pomiędzy dyskami twardymi, a nośnikami półprzewodnikowymi, różnią się też wykorzystywane w nich rozwiązania podsystemu translacji adresów logicznych na fizyczne.

Ponadto w miarę postępu technicznego następuje ewolucja oprogramowania układowego, obejmująca także podsystem translacji. Skutkuje ona różnicami w niuansach pomiędzy poszczególnymi rodzinami nośników nawet w ramach tej samej architektury oprogramowania układowego. Dlatego zagadnienie translacji adresacji logicznej na fizyczną należy do najbardziej skomplikowanych tematów dotyczących odzyskiwania danych.

Podsystem translacji był w miarę prosty w starszych generacjach dysków twardych, gdzie sprowadzał się do nadawania kolejnych numerów LBA fizycznym sektorom w oparciu o określony algorytm. Algorytmy tworzenia translatora komplikowały się w miarę postępów w optymalizacji wykorzystania powierzchni, implementacji stref o różnej liczbie sektorów na ścieżkę [Ruemmler, Wilkes 1994] oraz rozwoju metod zarządzania defektami. Względnie stałe przypisanie adresów LBA i prostota podsystemu translacji sprzyjały jego wysokiej niezawodności aż do czasu pojawienia się dysków z zapisem dachówkowym (SMR – *Shingled Magnetic Recording*) [Amer i in. 2011].

Zapis dachówkowy pozwala na zwiększenie gęstości zapisu przez częściowe nadpisanie, a tym samym zwężenie poprzedniej ścieżki przy zapisie następnej. Konsekwencją tej metody zapisu jest utrata możliwości przepisywania pojedynczych sektorów – ponieważ głowica zapisująca indukuje pole magnetyczne szerzej, niż wynosi szerokość ścieżki, taki zapis uszkadzałby zawartość sektorów na sąsiednich ścieżkach [Kanai i in. 2010]. Dlatego kiedy zachodzi potrzeba zmiany zawartości sektora, konieczne jest przepisanie całej grupy ścieżek. Takie przepisywanie całych grup ścieżek negatywnie wpływa na wydajność dysku przy zapisie.

Aby uniknąć tego efektu, producenci sięgają po różne metody optymalizacji zapisu. Ogólnie sprowadzają się one do zapisywania nowej zawartości sektorów LBA nie tam, gdzie te sektory się pierwotnie fizycznie znajdowały, ale tam, gdzie jest to w danej sytuacji najwygodniejsze. Oznacza to zerwanie stałego przypisania adresów logicznych do fizycznych sektorów i wymusza wzrost złożoności podsystemu translacji adresacji logicznej na fizyczną tak, aby na bieżąco śledził aktualne położenie adresów LBA w fizycznych sektorach.

Inaczej wygląda sytuacja w nośnikach półprzewodnikowych, gdzie brak możliwości bezpośredniego nadpisania istniejącej zawartości od początku wymusił rotację adresów LBA

po adresach fizycznych. Zawartość układów typu Flash nie może być zmieniona przez proste przeprogramowanie, ale wymaga uprzedniego skasowania zawartości i jej zaprogramowania na nowo. Dlatego pamięci Flash-NAND są podzielone na dwa rodzaje fizycznych jednostek alokacji: strony, jako jednostki programowania i odczytu oraz zawierające wiele stron bloki, jako jednostki kasowania.

Nośniki wykorzystujące pamięci tego typu zawsze utrzymują pewną liczbę wolnych, skasowanych bloków, aby te mogły być zaprogramowane nową zawartością. I kiedy zostaną zaprogramowane, w tablicach warstwy translacji Flash (*Flash Translation Layer* – FTL) [Chiang, Lee, Chang 1999] są im przypisywane odpowiednie adresy LBA. Jednocześnie z adresacji LBA są wyrzucane bloki zawierające przestarzałe dane, co pozwala na ich skasowanie i przygotowanie na przyjęcie następnych informacji.

To bardzo uproszczony model zarządzania translacją adresacji logicznej na fizyczną w nośnikach półprzewodnikowych. Ponieważ operacje programowania i kasowania zużywają układy Flash-NAND, co prowadzi do ich awarii, a ceną zwiększania gęstości zapisu jest spadek żywotności pamięci tego typu, producenci są zmuszeni rozwijać metody zarządzania defektami oraz ograniczania i wyrównywania zużycia. Jedną z najistotniejszych metod optymalizacji jest funkcja TRIM [Kaczmarzyk 2024f], która pozwala ograniczyć fizycznie przechowywaną informację jedynie do obszarów zaalokowanych w strukturach logicznych systemów plików.

Funkcja TRIM nie tylko pozwala ograniczyć zużycie układów Flash-NAND operacjami programowania i kasowania, ale też korzystnie wpływa na wydajność wykonywanych operacji. Z tego względu znalazła zastosowanie także w borykających się z problemem wydajności zapisu dyskach SMR. Jednak funkcja TRIM ma istotną wadę z punktu widzenia odzyskiwania danych i informatyki śledczej. Dane skasowane na poziomie struktur logicznych systemu plików niemal natychmiast przestają być dostępne w adresacji LBA i jedyną szansą na ich odzyskanie jest poszukiwanie ich w adresacji fizycznej.

Z uwagi na rosnącą złożoność i dynamikę zachodzących w podsystemie translacji zmian, jest on podatny na błędy i uszkodzenia. Problemy translatora są główną przyczyną awarii nośników półprzewodnikowych i bardzo istotną w przypadku dysków SMR. Ponieważ każdy egzemplarz nośnika danych ma pewne indywidualne cechy, jak np. liczba i rozmieszczenie defektów, każdy translator jest unikatowy i nie można go zastąpić innym, skopiowanym z innego nośnika.

2.5. Kodowanie i dekodowanie danych

Dane zapisane na nośnikach informacji są danymi przekształconymi w procesie kodowania i istotnie różnią się od tego, co użytkownik widzi w swoich plikach. Jest wiele powodów sprawiających, że dane na cyfrowych nośnikach informacji nie mogą być zapisywane w postaci surowego strumienia zer i jedynek tak, jak może je zobaczyć użytkownik w edytorze szesnastkowym. Do najważniejszych z nich należą konieczność zapewnienia spójności danych i korekcji możliwych błędów oraz dążenie do jak najefektywniejszego upakowania danych na nośniku.

Ponieważ na każdym etapie przechowywania i przesyłania danych istnieje ryzyko wystąpienia w nich błędów i przekłamań, szeroko wykorzystuje się różnego rodzaju sumy kontrolne (np. CRC – *Cyclic Redundance Code* – cykliczny kod nadmiarowy) i kody korekcji błędów (ECC – *Error Correction Code*) [Lin, Costello 1983, Moreira, Farrell 2006]. Rozwiązania tego typu stosuje

się zarówno w protokołach komunikacyjnych, jak i nośnikach danych. I o ile w przypadku protokołów komunikacyjnych są one opisane w stosownych standardach, w przypadku nośników informacji szczegóły ich implementacji zależą od producenta i architektury oprogramowania układowego, a nieraz można zauważyć pewne różnice w obrębie jednego modelu urządzenia z różnymi wersjami oprogramowania układowego.

W przypadku nośników półprzewodnikowych, do zapisywanych w stronach danych użytkownika dodawana jest też inna informacja nadmiarowa. W szczególności dotyczy to znaczników numerów logicznych bloków, czasem też numerów logicznych stron oraz liczników służących algorytmom wyrównywania zużycia do monitorowania zużycia poszczególnych bloków. Szczegóły tej informacji w dużym stopniu zależą od rozwiązań oprogramowania układowego zaimplementowanego w danym nośniku [Thirumalai 2023]. Rozmieszczenie danych użytkownika i informacji nadmiarowej w stronie nazywa się formatem strony.

Dane bardzo często są też randomizowane. Naturalne dane użytkownika często zawierają długie ciągi takich samych symboli lub powtarzalne wzorce. Tego typu dane, ze względu na odbicia fal, powstawanie fal stojących i pasożytnicze harmoniczne, są trudniejsze w bezbłędnym przesyłaniu, a ze względu na zjawiska indukcyjne, także w przechowywaniu. Dlatego, w celu zmniejszenia ryzyka wystąpienia bitowych błędów, są one przekształcane, zazwyczaj z wykorzystaniem funkcji logicznej alternatywy rozłącznej (XOR) i specjalnych, czasami generowanych dynamicznie szablonów.

Jednym z popularnych zabiegów związanych z kodowaniem danych jest ich szyfrowanie. Szyfrowanie powszechnie kojarzone jest z bezpieczeństwem danych i ich ochroną przed nieautoryzowanym dostępem, jednak popularność sprzętowego szyfrowania w nośnikach danych ma też drugie uzasadnienie. Algorytmy szyfrowania równocześnie bardzo dobrze randomizują dane i zwłaszcza w przypadku dysków SSD, można podejrzewać, że to jest główna przyczyna ich tak szerokiego rozpowszechnienia.

Z uwagi na to, że nośniki półprzewodnikowe ulegają zużyciu w wyniku operacji kasowania i programowania, producenci dążą do ograniczania liczby wykonywanych operacji tego typu. Jednym ze stosowanych przez nich zabiegów, jest wewnętrzna kompresja danych. W ten sposób zmniejsza się objętość zapisywanej informacji, a przy okazji ta informacja jest też randomizowana.

W nośnikach optycznych i magnetycznych dane są dodatkowo kodowane pod kątem optymalizacji gęstości upakowania danych. Pierwotną metodą kodowania danych w dyskach twardych była metoda FM (*Frequency Modulation* – modulacja częstotliwościowa). Polegała ona na zapisie sygnału zegarowego i umieszczaniu pomiędzy impulsami zegarowymi dodatkowych impulsów dla bitów o wartości „1”. Jeśli między impulsami zegarowymi nie było jedynki, oznaczało to logiczne zero.

Była to bardzo nieefektywna metoda kodowania, która stanowiła istotną barierę w rozwoju nośników magnetycznych. Dlatego z czasem była zamieniona metodą MFM (*Modified Frequency Modulation* – modyfikowana modulacja częstotliwościowa), w której ograniczono liczbę impulsów zegarowych. Jednak naprawdę istotne możliwości zwiększenia gęstości zapisu w dyskach twardych pojawiły się w konsekwencji opracowania płyt CD (*Compact Disc*).

Ponieważ w przypadku nośników optycznych łatwiej jest wykrywać zmianę fizycznego stanu medium, niż odróżniać odbicie światła od obszarów wypalonych i niewypalonych (pity

i landy), została dla nich opracowana metoda kodowania EFM (*Eight-to-Fourteen Modulation* – modulacja 8 do 14). Polegała ona na takim przekodowaniu danych, żeby zawsze pomiędzy jedynekami występowało co najmniej jedno zero. Powodowało to wydłużenie ciągu bitów (każdy 8-bitowy bajt rozrastał się do 14 bitów), ale jednocześnie ułatwiało upakowanie tych bitów w fizycznym medium [Schouhamer Immink 2004].

W tej metodzie kodowania łatwe do wykrycia impulsy oznaczają logiczne jedynki, a liczbę zer pomiędzy tymi jedynekami oblicza się na podstawie czasu, jaki upływa między poszczególnymi jedynekami. Wymaga to dokładnej kontroli prędkości obrotowej napędu, by zapewnić odczyt sygnału o stabilnej częstotliwości, ale pozwala upakować na nośniku więcej informacji przy danych fizycznych ograniczeniach. I na wzór wykorzystywanej w płytach CD metody EFM, została opracowana rodzina kodów RLL (*Run Length Limited* – ograniczona długość serii) wykorzystywana w dyskach twardych.

Kodowanie RLL pozwoliło zrezygnować z zegarowej składowej zapisywanego sygnału i uzyskać znaczny wzrost gęstości zapisu. Liczba zer, jakie mogą wystąpić pomiędzy dwiema jedynekami zależy głównie od możliwości utrzymania poprawnej synchronizacji sygnału, jego dekodowania oraz korekcji występujących błędów bitowych. Bardziej szczegółowy opis kodowania danych w dyskach twardych można znaleźć w [Vasić, Kurtas 2005].

2.6. Stany logiczne i fizyczne

Dane użytkownika, to logicznie interpretowany ciąg bitów – zer i jedynek, czyli stanów logicznych odczytywanych z fizycznego medium. Każdy stan logiczny jest interpretacją fizycznego stanu nośnika. To, czy dany stan fizyczny będzie logicznie interpretowany jako „0”, czy jako „1” zależy wyłącznie od przyjętej konwencji, podobnie, jak od konwencji zależy przypisanie ładunku ujemnego elektronowi, a dodatniego – protonowi. Gdyby te oznaczenia przypisano odwrotnie, fizyka by się od tego nie zmieniła, a jedynie zmieniłby się jej opis.

Podstawą logicznej interpretacji mogą być różne stany fizyczne zarówno stabilne (nośniki nieulotne – energoniezależne), jak i wymagające podtrzymywania zasilania (nośniki ulotne – energozależne). W przypadku nośników ulotnych nie ma możliwości odzyskiwania danych po odłączeniu ich od zasilania. Taka możliwość jest jedynie w przypadku, kiedy stany fizyczne pozostają stabilne niezależnie od zewnętrznego zasilania.

W nośnikach nieulotnych wykorzystuje się wiele fizycznych zjawisk, jakie można interpretować logicznie. Do najważniejszych należą namagnesowanie powierzchni (nośniki magnetyczne) i ładunki elektryczne zgromadzone w bramkach pływających tranzystorów (nośniki półprzewodnikowe). Wciąż jeszcze można spotkać nośniki optyczne wykorzystujące powierzchnię odbijającą lub rozpraszającą światło. Natomiast w przyszłości możemy się spodziewać nośników danych wykorzystujących zjawiska związane ze zmianą rezystancji.

Zapis w nośnikach magnetycznych polega na uporządkowaniu namagnesowania powierzchni magnetycznej [Кожаневский 2005]. Odczyt następuje przez przemieszczenie nośnika pod głowicą, w jakiej jest indukowany sygnał elektryczny. Impulsy indukowane w tym sygnale przez obszary zmiennego namagnesowania, to jest ściany domenowe, interpretowane są jako logiczne jedynki. Brak takich impulsów oznacza logiczne zera [Bertram 1994]. Dokładny sposób interpretacji sygnału zależy od szczegółów implementacji kodowania.

W przypadku nośników półprzewodnikowych wykorzystywane są zmodyfikowane tranzystory polowe typu NPN z kanałem zubażonym, gromadzące ładunki elektryczne w bramkach pływających. Ponieważ zgromadzony ładunek elektryczny zamyka kanał N, typowo naładowana bramka pływająca była interpretowana jako logiczne „0”, a pusta – jako „1”. Po wprowadzeniu technologii wielostanowej, pozwalającej przechowywać więcej, niż 1 bit w tranzystorze, interpretacja logiczna ładunku stała się bardziej skomplikowana. Wartość logiczna zależy od wartości napięcia przyłożonego między źródłem, a drenem niezbędnego dla otwarcia tranzystora [Michelsoni, Crippa, Marelli 2010].

Nośniki optyczne, to tłoczone lub wypalane płyty, gdzie na ścieżce naprzemiennie pojawiają się odcinki lepiej lub gorzej odbijające światło. Przetwornik rejestruje zmiany odbicia światła i te zmiany są interpretowane, jako logiczne jedynki. Układ dekodera wylicza liczbę zer pomiędzy jedynkami na podstawie czasu, jaki upływa między wystąpieniem kolejnych jedynek w sposób opisany w sekcji dotyczącej kodowania danych [Mansuripur, Sincerbos 1997].

W przyszłości popularność mogą zyskać nośniki oparte o zjawiska związane ze zmianą rezystancji. Typowo w pamięciach tego typu logiczną jedynką jest stan niskiej, a zerem – wysokiej rezystancji. Do najbardziej perspektywicznych należą już przetestowane w realnie działających urządzeniach pamięci zmiennofazowe (PCM – *Phase Change Memory*), a także pamięci magnetorezystywne (MRAM – *Magnetic Random Access Memory*).

Pamięci zmiennofazowe wykorzystują chalcogenki – substancje, jakie mogą występować w postaci krystalicznej lub amorficznej (nieregularnej, podobnej do szkła). Jeśli chalcogenek podgrzać, a następnie powoli wystudzić, uzyskamy kryształ o niskiej rezystancji. Jeżeli chalcogenek zostanie wystudzony gwałtownie, nie zdąży wykryształizować i zastygnie w postaci amorficznej, o wysokiej rezystancji [Redaelli 2018].

Koncepcje wykorzystania zjawisk magnetorezystywnych do przechowywania danych pojawiły się już w latach '70, jednak zostały zarzucone jako mało perspektywiczne. Wszystko zmieniło się po odkryciu zjawisk gigantycznego i tunelowego magnetooporu, które nadały pracom nad pamięciami magnetorezystywnymi nowy impuls. Istota koncepcji sprowadza się do wykorzystania dwóch warstw substancji magnetycznych namagnesowanych w taki sam sposób (równolegle) lub przeciwnie (antyrownolegle). W przypadku polaryzacji równoległej rezystancja jest znacząco niższa, niż w przypadku antyrownoległej, co daje podstawę do wyróżnienia stanów logicznych [Dieny, Goldfarb, Lee 2017].

Prócz tego prowadzone są prace nad pamięciami elektrochemicznymi, w których za zmianę rezystancji odpowiadają procesy redukcji i utleniania metali. Metale mają znacznie niższą rezystancję od ich tlenków, co pozwala na przypisanie im różnych wartości logicznych [Nishi 2014]. Jeszcze jednym przykładem pamięci rezystywnych mogą być nanorurki węglowe i budowane z nich struktury o różnej rezystancji [Ning, Luo 2019].

3. Przyczyny utraty i możliwości odzyskania danych

Utrata dostępu do danych może być spowodowana różnymi czynnikami. Różne typy nośników różnią się wrażliwością na różne rodzaje uszkodzeń oraz możliwościami odzyskania danych. Przy czym nie w każdym przypadku, kiedy odzyskiwanie danych zakończy się niepowodzeniem z powodu przeszkód praktycznych, oznacza to, że ich odzyskanie jest w ogóle

niemożliwe. W dalszej części zostaną wskazane najistotniejsze przyczyny utraty dostępu do informacji, metody ich diagnostyki oraz sposoby odzyskiwania danych.

3.1. Uszkodzenia elektroniczne

Uszkodzenia elektroniczne najczęściej są wynikiem podłączenia nośnika danych do nieprawidłowego zasilania. Skutki tego typu uszkodzeń typowo ograniczają się do uszkodzenia elementów nieistotnych dla przechowywania danych i na ogół łatwych do wymiany, jak bezpieczniki, diody Zenera, czy rezystory. Dlatego w większości wypadków dla odzyskania dostępu do danych wystarczające jest naprawienie urządzenia.

Usterki elektroniczne na ogół można dość łatwo zidentyfikować. Urządzenia z uszkodzeniami tego typu nie uruchamiają się, nie reagują na zasilanie lub wykazują objawy typowe dla zwarcia, jak silnie grzejące się elementy i wysoki pobór prądu, co często prowadzi do odłączenia zasilania lub zadziałania zabezpieczeń przeciwprzeciążeniowych i przeciwzwarciowych. Uszkodzone elementy (przepalone bezpieczniki i rezystory, przebite diody i kondensatory) można znaleźć używając miernika.

Jeśli nośnik uruchamia się z typowym dla niego poborem prądu i normalnie obciąża magistralę, nawet jeśli nie jest rozpoznawany przez BIOS lub system operacyjny, uszkodzenie elektroniczne można z prawdopodobieństwem graniczącym z pewnością wykluczyć. W szczególności praktycznie wykluczyć uszkodzenie elektroniczne dysków twardych pozwala uruchomienie silnika i rozpędzenie talerzy. W przypadku dysków SSD warto sprawdzić temperaturę pracy kontrolera i porównać ją z temperaturą pracy sprawnego podobnego dysku na takim samym kontrolerze. W zależności od modelu kontrolera, jego normalna temperatura pracy może wynosić od ok. 30 do ponad 60 °C.

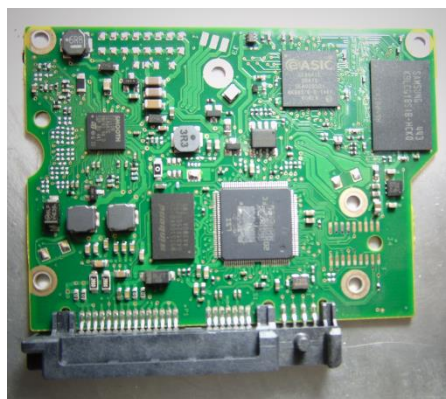
W niektórych wypadkach uszkodzenia okazują się rozleglejsze i w przypadku dysków twardych zasadną staje się wymiana elektroniki na sprawną. Trzeba przy tym pamiętać, że czasy, kiedy wystarczało proste przełożenie takiej samej (niekoniecznie pochodzącej od tego samego modelu – te same elektroniki są wykorzystywane w całych rodzinach modeli) płytki elektroniki minęły ok. 20 lat temu. Rozwojowi dysków twardych towarzyszył także rozwój oprogramowania układowego i wzrost znaczenia indywidualnie programowanych parametrów. Dlatego obecnie konieczne jest przelutowanie na elektronikę dawcy zawierającego część oprogramowania układowego EEPROMu (*Electrically Erasable Programmable Read-Only Memory*) pacjenta.

EEPROM zwykle jest w układzie scalonym w obudowie typu SOP-8 (*Small Outline Package 8*). W niektórych wypadkach można spotkać więcej, niż jedną pamięć tego typu – wtedy oczywiście należy przelutować wszystkie. W innych modelach zdarza się, że EEPROM jest integrowany wewnątrz procesora sygnałowego. W takich sytuacjach konieczne jest przelutowanie procesora sygnałowego lub odczytanie jego zawartości i zaprogramowanie procesora na innej elektronice. W przypadku uszkodzenia procesora sygnałowego zawierającego wewnętrzny EEPROM, i tak warto podjąć próbę odczytania zawartości EEPROMu. Takie próby często kończą się powodzeniem, nawet w przypadku układów scalonych z wypalonymi dziurami.

Utrata zawartości EEPROMu może skomplikować, a w wielu przypadkach praktycznie uniemożliwić odzyskanie dostępu do zawartości, chociaż ona cały czas istnieje na dysku. Dla części modeli dysków istnieją metody pozwalające na odbudowę zawartości EEPROMu i odzyskanie danych, jednak np. dla Seagateów pokolenia F3, czyli dla architektury obecnej na rynku

od ponad 15 lat takiej metody nie ma. Opracowanie takiej metody prawdopodobnie jest możliwe, ale wymagałoby oscyloskopowych badań sygnału przechwytywanego bezpośrednio z bloku głowic magnetycznych. Praktycznie uniemożliwić dostęp do danych może także utrata kluczy szyfrujących, jakie mogą być zapisane w EEPROMie przejściówki USB-SATA dysków zewnętrznych lub w procesorach sygnałowych niektórych dysków twardych (np. dysków WD z rodzin *Spyglass*).

Specyficzną dla dysków SSHD (*Solid State Hybrid Drive*) kategorią uszkodzeń są usterki bufora Flash-NAND. Dyski SSHD są to dyski twarde wyposażone w dodatkowy bufor Flash-NAND o pojemności typowo 4–8 GB, służący do przechowywania zawartości najczęściej odczytywanych sektorów, w tym sektorów strefy serwisowej. Nie jest to uszkodzenie typowo elektroniczne – najczęściej wynika z zużycia układu Flash-NAND i pojawienia się błędów w jego zawartości.



Zdj. 1. PCB dysku SSHD

Objawem tej usterki jest brak reakcji na zasilanie w wyniku problemów w komunikacji z buforem, jednak w tym wypadku żadne elementy elektroniczne nie są uszkodzone. W części przypadków pomaga wyczyszczenie zawartości i inicjalizacja bufora, jednak najczęściej konieczna jest wymiana całej elektroniki. Ponieważ bufor elektroniki pobrany od dawcy będzie zawierał informację serwisową niezgodną z pacjentem, konieczne jest jego wyczyszczenie i inicjalizacja. Podobnie, jak i w innych sytuacjach wymiany elektroniki, potrzebne jest przelutowanie oryginalnego EEPROMu.

W praktyce informatyki śledczej częściej, niż w typowych sytuacjach naturalnych usterek, można spotkać nośniki uszkodzone celowo. W przypadku usterek elektronicznych, celowe uszkodzenia najłatwiej spowodować podłączając urządzenie do zasilacza podającego wyższe napięcie lub zalewając urządzenie różnymi płynami. Uszkodzenia powodowane pierwszym z tych sposobów na ogół mało różnią się od naturalnych usterek. W razie wykrycia śladów zalania, w pierwszej kolejności należy wyczyścić substancję, jaką urządzenie zostało zalane, usunąć ślady korozji i dopiero wtedy przystąpić do dalszej diagnostyki. W przypadku podejrzenia, że płyn mógł dostać się do wnętrza hermobloku dysku twardego, przed jego uruchomieniem należy sprawdzić jego stan wewnątrz i w razie potrzeby wyczyścić talerze oraz dokonać niezbędnych napraw podsystemu mechanicznego.

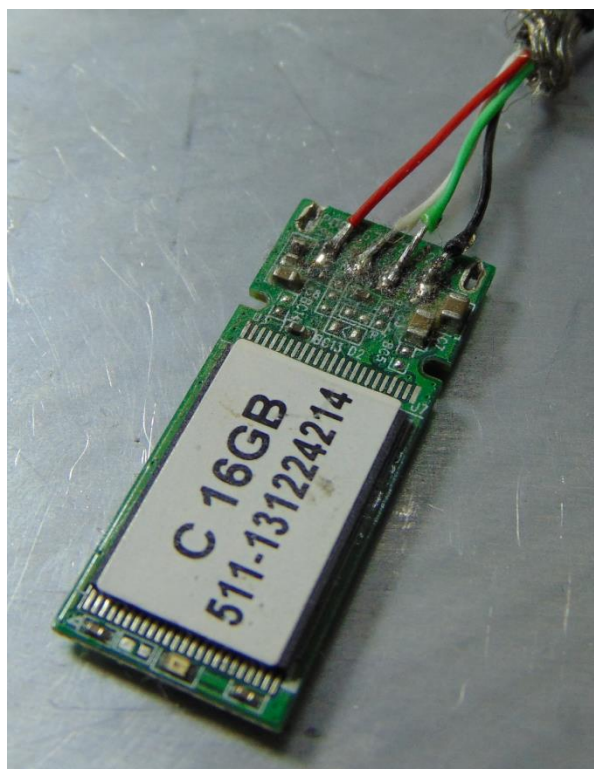
O ile w przypadku dysków twardych wymiana PCB (*Printed Circuit Board*) na sprawną jest na ogół prostym, tanim i skutecznym sposobem naprawy usterek elektronicznych, w przypadku nośników półprzewodnikowych oraz urządzeń z wbudowaną pamięcią typu Flash (np. eMMC

– *embedded MultiMedia Card* lub MCP – *Multi Chip Package*), naprawa przez prostą wymianę części nie wchodzi w grę. Dlatego w wypadku urządzeń tego typu należy w pierwszej kolejności dążyć do przywrócenia im pełnej sprawności. Jeśli z jakiegoś powodu (np. uszkodzenia laminatu, nadmiernie rozwinięta korozja) [Pawlikowski 2023] jest to niemożliwe, kolejnym wariantem odzyskiwania danych jest wylutowanie układów pamięci, odczyt ich zawartości na programatorze i dalsza analiza binarnych obrazów metodami analogicznymi, jak dla uszkodzeń oprogramowania układowego ze wszystkimi ich ograniczeniami.

Ze względu na te ograniczenia, a zwłaszcza szyfrowanie, często odczyt zawartości układów pamięci nie może w praktycznych sytuacjach doprowadzić do odzyskania zawartości. Dlatego w pewnych sytuacjach zasadnym jest przelutowanie kontrolera i układów pamięci na inną PCB. Przy tym przelutowanie samych układów pamięci jest obciążone wysokim ryzykiem zniszczenia ich zawartości w wyniku ich inicjalizacji przez obcy kontroler. Także w przypadku urządzeń mobilnych, IoT i podobnych konieczne jest przelutowanie ich procesorów lub kontrolerów oraz EEPROMów, m. in. ze względu na to, że te układy mogą przechowywać klucze szyfrujące niezbędne dla odszyfrowania zawartości.

3.2. Uszkodzenia mechaniczne

Uszkodzenia mechaniczne nośników danych zasługują na szczególną uwagę, gdyż są one łatwe do szybkiego celowego spowodowania, np. w sytuacji zatrzymania podejrzanego. Z uwagi na ich konstrukcję dyski twarde są o wiele bardziej podatne na usterki mechaniczne, niż nośniki półprzewodnikowe. W przypadku tych ostatnich najczęściej można spotkać relatywnie proste do identyfikacji i usunięcia usterki, jak np. wyłamanie złącz. Takie uszkodzone złącza można wymienić, a w przypadku uszkodzenia laminatu PCB – ominąć wlutowując się przewodami za uszkodzeniem.



Zdj. 2. Przewód wlutowany w miejsce uszkodzonego złącza USB

3.2.1. Mechaniczne uszkodzenia nośników półprzewodnikowych

Realne mechaniczne zniszczenie danych na nośnikach półprzewodnikowych jest możliwe tylko poprzez uszkodzenie wszystkich układów Flash-NAND wchodzących w skład takiego nośnika. Przy czym kryształy pamięci zajmują jedynie część układu scalonego i nie każde uszkodzenie uniemożliwia odzyskanie danych. Dlatego warto podjąć próbę odczytania układów, jeśli są one uszkodzone w niewielkim stopniu i można z nimi nawiązać komunikację.

W przypadku układów ukruszonych zdarza się, że pracują one niestabilnie i łatwo się przegrzewają, co wymaga chłodzenia ich podczas odczytu, a często też wielokrotnych prób odczytu. Uszkodzone wyprowadzenia można regenerować lub zastępować przylutowując układ bezpośrednio do wyprowadzeń programatora albo odpowiedniego adaptera. Osobnym zagadnieniem jest możliwość praktycznego zdekodowania pozyskanych obrazów binarnych i poprawnego złożenia obrazu struktury logicznej. Ten proces może się zakończyć niepowodzeniem nie tylko z powodu błędów lub niekompletności odczytu, ale też np. z powodu szyfrowania.

W przypadku poważniejszych uszkodzeń, jak złamanie układu, nie istnieją praktyczne metody odzyskania danych. Takie metody jednak mogą powstać w przyszłości. Złamany układ wciąż zawiera ładunki elektryczne, które mogą być obrazowane przy pomocy mikroskopów sił atomowych i badania w tym kierunku już są prowadzone [De Nardi i in. 2005, Hanzii i in. 2013].

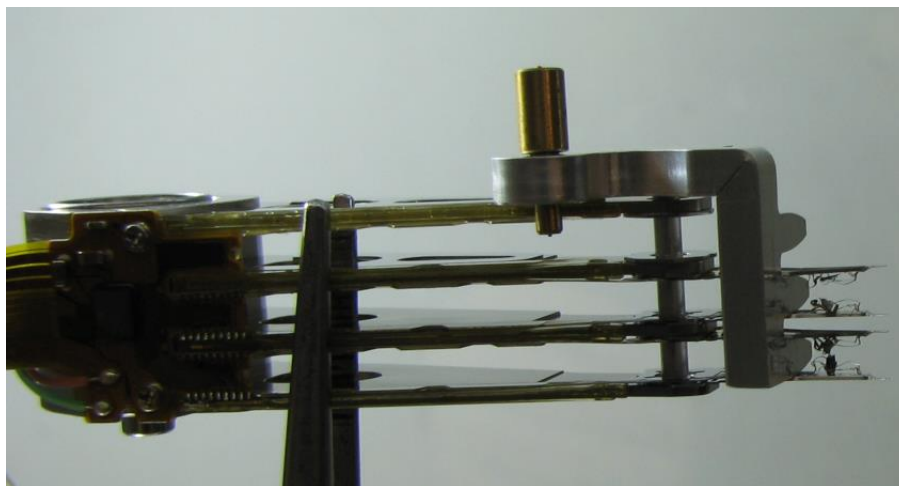
Odzyskanie danych w ten sposób wymaga odpowiedniej obróbki mechanicznej i chemicznej układu tak, żeby umożliwić zobrazowanie zgromadzonych w bramkach pływających ładunków elektrycznych. W przypadku układów wielowarstwowych konieczne jest powtórzenie tej operacji i zobrazowanie każdej warstwy. Dalej trzeba zinterpretować zgromadzone ładunki jako odpowiednie stany logiczne, a następnie zdekodować zawartość i złożyć w obraz struktury logicznej.

Przedstawiona wyżej metoda wciąż nie została dopracowana do końca, jednak przeprowadzone badania wykazały, że odzyskiwanie danych w ten sposób jest fizycznie wykonalne. Trzeba przy tym liczyć się z szeregiem praktycznych przeszkód związanych z wielowarstwowymi konstrukcjami układów scalonych, coraz mniejszymi rozmiarami tranzystorów oraz przechowywaniem wielu bitów w pojedynczych tranzystorach. Nie mniej istotne mogą okazać się zagadnienia związane z dekodowaniem, korekcją błędów i adresowaniem danych, a w wielu przypadkach też z ich odszyfrowaniem. Dlatego nawet, jeśli ta metoda zostanie dopracowana do końca, nie w każdym praktycznym przypadku okaże się skuteczna.

3.2.2. Uszkodzenia mechaniczne dysków twardych

3.2.2.1. Uszkodzenia bloków magnetycznych głowic

Najbardziej złożone usterki mechaniczne można spowodować w dyskach twardych. Najczęściej uszkodzeniu ulegają bloki magnetycznych głowic, a dokładniej – ślizgacze – sprężyste końcówki ramion, na których umieszczane są głowice. Stabilność odczytywanego sygnału w dyskach twardych zależy głównie od stabilności wysokości lotu głowic nad powierzchniami talerzy. Wysokość ta zależy od równowagi pomiędzy aerodynamiczną siłą nośną wytwarzaną przez ruch powietrza wywołany obracającymi się talerzami, a siłą sprężystości dociskającą ślizgacze do powierzchni talerzy [Коженевский 2009].



Zdj. 3. Urwane głowice

Jeśli dojdzie do uderzenia lub upadku dysku, ślizgacze podlegają dużemu przeciążeniu, które łatwo może doprowadzić do ich odkształcenia, co z kolei przekłada się na zmianę ich aerodynamicznej charakterystyki. W konsekwencji zmienia się wysokość lotu głowic nad powierzchniami talerzy i parametry odczytywanego przez nie sygnału, przez co procesor sygnałowy traci możliwość poprawnej interpretacji sygnału.

Ponieważ głowice odczytują nie tylko dane użytkownika, ale także sygnał serwo [Mamun, Guo, Bi 2006, Chen i in. 2006, Коженевский 2007] pozwalający ustalić aktualne położenie głowic nad powierzchnią talerza, odkształcenie ślizgaczy uniemożliwia poprawne odczytanie też tego sygnału [Wu 2000]. I właśnie utrata możliwości interpretacji sygnału serwo oraz określenia położenia głowic jest przyczyną najbardziej typowego objawu uszkodzenia mechanicznego – charakterystycznego stukania głowicami. Objaw ten wynika z ruchu głowic od ogranicznika do ogranicznika w poszukiwaniu ścieżek strefy serwisowej – obszaru zawierającego część oprogramowania układowego niezbędną dla dokończenia procesu inicjalizacji.

Stukanie głowicami jest bardzo typowym objawem uszkodzeń mechanicznych, ale może też wynikać z innych powodów. Objaw ten pojawi się też w przypadku zdemagnetyzowania (zniszczenia sygnału zapisanego na dysku przy pomocy pola magnetycznego) lub próby uruchomienia dysku z nieoryginalnym EEPROMem zawierającym parametry wzmocnienia sygnału nieodpowiadające danemu dyskowi. W rzadszych wypadkach gubienie sygnału i wchodzenie w stuk może też wynikać z innych problemów związanych z oprogramowaniem układowym.

Innym objawem wskazującym na problemy mechaniczne są nieudane próby rozpędzenia silnika. Najczęściej wynikają one z zaparkowania głowic na powierzchniach talerzy. Ponieważ zarówno głowice, jak i powierzchnie talerzy wykonywane są w taki sposób, żeby były jak najgładsze i jak najmniej zaburzały ruch powietrza wewnątrz hermobloku oraz minimalizowały ryzyko kontaktu [Li i in. 2005], jeśli dojdzie do zaparkowania głowic poza rampą lub strefą parkowania, pomiędzy nimi, a powierzchniami talerzy pojawiają się wiązania chemiczne, jakie blokują rozpędzenie talerzy.



Zdj. 4. Głowice zaparkowane na talerzu

3.2.2.2. Uszkodzenia silników

Znacznie rzadszymi przyczynami niemożności rozpędzenia silnika są zablokowane (zaklinowane) łożyska [Коженевский, Прокопенко, Гайшинец 2008] lub uszkodzenie uzwojeń silnika. Zaklinowanie łożyska było dosyć popularną usterką w dyskach, w których stosowano łożyska kulkowe, jednak ponad 20 lat temu spopularyzowały się znacznie bardziej odporne na uszkodzenia łożyska hydrodynamiczne i ten rodzaj uszkodzeń praktycznie zanikł. Do bardzo rzadkich należą też uszkodzenia uzwojeń silnika.

Żeby zdiagnozować uzwojenia, należy zmierzyć ich rezystancję. W zależności od modelu dysku, powinna ona wynosić od kilku do kilkudziesięciu Ω . Ogólnie w starszych dyskach można się spodziewać wyższej rezystancji, niż w nowszych, w dyskach 3,5" wyższej, niż w 2,5" i wyższej w dyskach z większą liczbą talerzy, niż z mniejszą. W przypadku przerywania uzwojenia miernik wykaże brak przejścia, a w przypadku zwarcia – rezystancję 0 Ω . W razie wątpliwości najlepiej zmierzyć rezystancję podobnego sprawnego dysku i porównać z wynikiem pacjenta.

3.2.2.3. Metody naprawy uszkodzeń mechanicznych

Typowe metody naprawy uszkodzeń mechanicznych polegają na wymianie uszkodzonych podzespołów na sprawne [Коженевский 2002]. Zazwyczaj wymieniane są bloki magnetycznych głowic. Przekładanie talerzy do innego korpusu ma sens jedynie w przypadku uszkodzeń silnika i wbrew obiegowym przekonaniom, nie należy tego robić poza sytuacjami, kiedy jest to naprawdę konieczne.

Najczęstszym praktycznym problemem w naprawie uszkodzeń mechanicznych jest dostępność odpowiednich dawców podzespołów. Z uwagi na brak możliwości zakupu potrzebnych części, konieczne jest kupowanie odpowiednich dysków – dawców, a w skrajnych sytuacjach wykorzystanie bloków magnetycznych głowic pochodzących z uszkodzonych dysków [<https://kaleron.edu.pl/vykorystannia-poszkodzenykh-blokov-magnitnykh-holovok-u-vidnovlenni-danykh.php>]. Zagadnienie odpowiedniego doboru dawców jest opracowane bardzo fragmentarycznie i niedokładnie. Przy ich doborze można kierować się udostępnianymi w Internecie wskazówkami, jednak w praktyce często okazuje się, że głowice w teorii jak najbardziej odpowiednie dla danego

pacjenta nie chcą poprawnie czytać sygnału, a głowice pobrane w desperacji z modelu ledwie tylko podobnego pozwalają skutecznie odzyskać dane.

Trudności w doborze dawców głowic zwiększa polityka producentów, potrafiących nierzadko pod tą samą nazwą handlową sprzedawać różne pod względem technicznym modele dysków. Z drugiej strony zmiennosc podzespołów pomiędzy pozornie bardzo różnymi modelami dysków wskazuje, że czasami na oznaczenia modeli większy wpływ ma marketing i segmentacja rynku, niż realne czynniki techniczne. Dodatkowym problemem jest odejście producentów od zwyczaju stosowania oznaczeń wskazujących na użyte w konstrukcji podzespoły lub niekonsekwentne używanie tych oznaczeń. Z tego względu dla weryfikacji poprawności doboru dawcy nieraz konieczne jest przełożenie głowic, a ewentualne niepowodzenie często zamiast odpowiedzi rodzi pytanie, czy głowice faktycznie są nieodpowiednie, czy może problemy z odczytem sygnału wynikają z innej przyczyny.

3.2.2.4. Spin-Stand

Powyższe trudności zostały zauważone już dawno temu i stały się podstawą opracowania koncepcji odzyskiwania danych niezależnie od dysku. Koncepcja ta opiera się o urządzenie pozwalające na zamontowanie talerza w specjalnym urządzeniu (*spin-stand*) i odczytaniu sygnału przy pomocy uniwersalnej głowicy, a następnie zdekodowaniu i interpretacji tego sygnału z wykorzystaniem odpowiedniego oprogramowania emulującego pracę oprogramowania układowego dysku. Wykonalność takiego procesu została potwierdzona praktycznie w 2006 r. [Sobey 2006].

Badania w tym kierunku, choć objęły również próby odzyskiwania w ten sposób nadpisanych danych [Mayergoyz, Tse 2007] były jednak rozwijane tylko przez bardzo krótki czas i dotyczyły jedynie dysków już wówczas bardzo starych i stanowiących bardzo proste konstrukcje, nawet w porównaniu do ówczesnych modeli. Życie pokazało, że odzyskiwanie danych w ten sposób, wprawdzie możliwe, jednak jest bardzo skomplikowane i wymagające pod kątem kompetencji technicznych, w szczególności w zakresie przetwarzania sygnału, metod kodowania danych oraz rozwiązań oprogramowania układowego dotyczących zarządzania defektami i adresacją. W połączeniu z kosztowną aparaturą, takie podejście nie było w stanie ekonomicznie konkurować z tradycyjnymi, wprawdzie nie wolnymi od problemów, ale prostszymi i tańszymi metodami.

Ewentualne próby opracowania metody odzyskiwania danych niezależnie od dysku ze współczesnych napędów musiałyby uwzględnić szereg dodatkowych komplikacji związanych z wprowadzeniem zapisu prostopadłego [Khizroev, Litvinov 2004], który pozwoliłby na uzyskanie większej gęstości zapisu przy jednoczesnym istotnym pogorszeniu stosunku sygnału do szumu. Także postępy w konstrukcji głowic [Mallinson 2002, Jiang i in. 2023] i ich pozycjonerów [Du, Pang 2019] oraz pojawienie się zapisu dwuwymiarowego (TDMR – *Two Dimensional Magnetic Recording*) [Chan i in. 2010, Khatami, Vasić 2013] stawiają pod znakiem zapytania możliwość stworzenia urządzenia naprawdę uniwersalnego, które byłoby w stanie zapewnić możliwość odczytu danych z talerzy pochodzących z dowolnych dysków.

Dodatkowymi problemami w opracowaniu uniwersalnego urządzenia są mimośrodowość, jaka pojawia się przy przełożeniu talerza do innego podsystemu mechanicznego oraz konieczność eliminowania efektów skosu [Miura i in. 2011, Hwang i in. 2015] w dyskach o wysokiej gęstości zapisu. Ponieważ nie jest technicznie możliwe dostatecznie precyzyjne złożenie dysku, by uniknąć

mimośrodowości, sygnał serwo jest zapisywany już po mechanicznym złożeniu dysku [Uematsu, Fukushi 2001, Yamada i in. 2006]. Późniejsze naruszenie położenia talerza względem osi silnika skutkuje trudnościami w śledzeniu ścieżki i jej częste gubienie, co znacząco wydłuża czas wykonywanych operacji.

3.2.2.5. Zanieczyszczenia i zarysowania powierzchni nośników danych

Innym problemem o charakterze mechanicznym jest zanieczyszczenie lub zarysowanie nośnika. W przypadku chronionych metalowymi obudowami dysków twardych tego typu problemy mogą wynikać z odkształcenia ślizgaczy powodującego kontakt głowic z powierzchniami talerzy lub z nieumiejętnych ingerencji w podsystem mechaniczny, przeprowadzanych przez niekompetentne osoby w nieodpowiednich warunkach. W przypadku nośników optycznych, jak płyty CD i DVD, zanieczyszczenie i zarysowanie nośnika najczęściej wynika z niewłaściwego sposobu przechowywania i narażenia ich na oddziaływanie czynników zewnętrznych. Znacznie rzadziej tego typu problemy są powodowane przez zdarzenia losowe, np. zalania.

Zanieczyszczone nośniki, w celu uniknięcia ich dalszej degradacji, należy przed podjęciem próby odzyskiwania danych wyczyścić. Dobór metody i środków czyszczących zależy od rodzaju zanieczyszczenia. Należy przy tym minimalizować ryzyko mechanicznej lub chemicznej degradacji nośnika.

W przypadku zarysowań, praktyczne metody odzyskiwania danych są silnie uzależnione od charakteru i skali uszkodzeń. W przypadku dysków twardych nawet niewielkie zarysowania mogą być pogłębione i poszerzone przez kontakt głowicy z powierzchnią talerza. Każda nierówność powierzchni może spowodować utratę przez ślizgacz siły nośnej, co spowoduje dociśnięcie go do powierzchni talerza i kontakt, jaki może spowodować jej dalsze uszkodzenie. W rezultacie często nawet niewielkie zarysowania przerastają w zapiły cylindryczne – charakterystyczne okręgi zapiłowane w powierzchni talerza. Pojawienie się zapiłu cylindrycznego może łatwo uniemożliwić odzyskanie danych jeśli nie z całego dysku, to co najmniej z zarysowanej powierzchni.



Zdj. 5. Zapił cylindryczny

Kiedy głowica znajdzie się nad zapiłem, będzie wpadała do środka i uderzała o powierzchnię powodując jej dalsze uszkodzenie przez pogłębienie i poszerzenie zapiłu. Odbijając się od powierzchni talerza, ślizgacz wchodzi w vibrację, co prowadzi do dalszych kontaktów

z powierzchnią. Głowica uszkadza się mechanicznie i termicznie od tarcia o uszkodzoną powierzchnię, jednocześnie wybierając z niej materiał, który powoduje zanieczyszczenie wnętrza hermobloku.

Pogłębienie zapilu utrudnia, a czasami uniemożliwia wyprowadzenie z niego głowic, a unoszące się wewnątrz hermobloku opiłki metalu sprzyjają degradacji pozostałych powierzchni. W ten sposób łatwo może dojść do pojawienia się symetrycznych zapilów na wszystkich powierzchniach i praktycznego uniemożliwienia odzyskania danych. W skrajnym przypadku uruchomienie uszkodzonego w ten sposób lub zanieczyszczonego wewnątrz dysku może doprowadzić do całkowitego zeszlifowania powierzchni magnetycznej, co uniemożliwi odzyskanie danych nie tylko praktycznie, ale też fizycznie.

Dla dysków optycznych zostały opracowane metody ich czyszczenia, szlifowania, wypełniania zarysowań, wyrównywania powierzchni oraz polerowania [Ташиков 2010]. W przypadku dysków twardych takie podejście, z uwagi na znacznie większą gęstość zapisu, jest znacznie trudniejsze. Ponadto zależność parametrów sygnału magnetycznego od odległości przechwytyjących ten sygnał głowic wpływa na możliwości jego interpretacji przez procesor sygnałowy. Dlatego jakiegokolwiek próby wyrównywania powierzchni, wypełniania zarysowań, czy nanoszenia warstwy ochronnej na powierzchnię talerza dysku twardego wymagałyby uwzględnienia w oprogramowaniu układowym zmian odległości głowicy od warstwy magnetycznej i odpowiedniej korekty wzmocnienia sygnału.

3.2.2.6. Metody obrazowania powierzchni nośników danych

Wszystkie praktycznie stosowane metody odzyskiwania danych z dysków twardych oraz płyt nośników optycznych wymagają wprowadzenia nośnika w ruch obrotowy. Oznacza to, że uszkodzenia uniemożliwiające wprowadzenie nośnika w ruch obrotowy, jak złamanie, wygięcie, czy przedziurawienie, w praktyce uniemożliwia odzyskanie danych, chociaż w fizycznym sensie wciąż są one w dużym stopniu odzyskiwalne. Aby dane z tak uszkodzonych nośników odzyskać, konieczne jest zobrazowanie ich powierzchni, a następnie pozyskanie na podstawie obrazu zapisanego sygnału i jego zdekodowanie.

Przy tym w przypadku nośników optycznych konieczne jest zobrazowanie wypalonych (lub wytłoczonych) i niewypalonych (niewytłoczonych) fragmentów ścieżki, a w nośnikach magnetycznych – namagnesowania powierzchni. Dlatego dla uszkodzonych płyt CD i DVD zasadnym jest obrazowanie z użyciem mikroskopów optycznych, a dla dysków twardych – mikroskopii sił magnetycznych. Nie znaczy to, że w przeszłości nie podejmowano prób odtwarzania namagnesowania powierzchni przy pomocy środków optycznych [Коженевский 2004].

Przez dziesięciolecia do obrazowania namagnesowania powierzchni używano, opracowaną przez Francis Bittera na początku lat '30, metodę wykorzystującą koloidową zawiesinę zawierającą cząstki magnetytu [Bitter 1932]. Po naniesieniu zawiesiny na namagnesowaną powierzchnię cząstki magnetytu zbierają się wzdłuż ścianek domenowych pozwalając obserwować położenie domen magnetycznych przy pomocy mikroskopu optycznego. Ograniczeniem jest rozdzielczość mikroskopów optycznych, która jeszcze w latach '90, przy rosnącej gęstości zapisu na dyskach twardych, okazała się niewystarczająca.

Inna koncepcja zakładała wykorzystanie magnetooptycznych efektów Kerra i Faradaya polegających na odchyleniu spolaryzowanego światła pod wpływem pola magnetycznego

[Коженевский i in. 2003]. Przy czym efekt Kerra obserwowany jest przy odbiciu światła od namagnesowanej powierzchni, a efekt Faradaya – przy przejściu przez namagnesowany ośrodek. Dlatego w przypadku nośników magnetycznych efekt Kerra można obserwować bezpośrednio, a obserwacja efektu Faradaya wymaga użycia przezroczystego ośrodka o właściwościach ferromagnetycznych – kryształu ferrogranatu [Агалиди i in. 2012]. Jednak rozdzielczość i tych metod przestała być wystarczająca dla dysków twardych już w latach '90.

Dlatego jedyną racjonalną metodą dla odzyskiwania danych z poważnie uszkodzonych talerzy dysków twardych jest mikroskopia sił magnetycznych. Historia badań dysków twardych z użyciem mikroskopów sił magnetycznych sięga przełomu lat '80 i '90 [Gomez i in. 1992, Gomez i in. 1993] i pierwotnie badania te były ukierunkowane na odzyskanie nadpisanych danych. Ostatecznie badania wykazały brak możliwości odzyskania nadpisanych danych [Wright, Kleiman, Shyaam Sundhar 2008], ale potwierdziły praktyczną możliwość odzyskiwania danych z talerzy uszkodzonych mechanicznie, w tym rozdrobnionych specjalnymi niszczarkami do niszczenia dysków [Hughes, Commins, Coughlin 2009].

Obrazowanie namagnesowanej powierzchni jest tylko pierwszym krokiem procesu odzyskiwania danych. Później jeszcze trzeba pozyskane obrazki graficzne przedstawiające namagnesowanie fragmentów talerza złożyć w całość i dopiero na tej podstawie przeprowadzić analizę sygnału. Im więcej takich fragmentów, tym bardziej złożone zadanie, zwłaszcza, jeśli wśród obrazowanych fragmentów znajdują się też pochodzące od innych dysków.

I to złożoność zadania obejmującego odseparowanie fragmentów właściwego dysku od pochodzących z innych nośników sprawia, że jest skrajnie mało prawdopodobne, by kiedykolwiek praktycznie odzyskano dane ze zmielonego dysku. Natomiast całkiem realne jest odzyskanie danych z dysków uszkodzonych w delikatniejszy sposób, np. przy zarysowaniach i zapiłowaniach powierzchni powodujących uszkodzenie głowic przy próbach odczytania danych tradycyjną metodą. Dotyczy to także dysków uszkodzonych celowo, np. przewierconych, przebitych gwoździami, rozbitych młotkiem, z wygięciami lub pęknięciami talerzy spowodowanymi wkręceniem w odpowiednie miejsce obudowy długiej śruby (tzw. metoda „czerwonej kropki” [Sołodow 2018]) lub w inny sposób.

3.3. Uszkodzenia oprogramowania układowego

Jeszcze 20 lat temu uszkodzenia oprogramowania układowego nośników danych należały do rzadkości. Od tamtego czasu jednak wiele się zmieniło, a postęp techniczny wymusił znaczny wzrost złożoności oprogramowania układowego, co przyczyniło się do wzrostu jego podatności na awarie. Szczególnie istotnie znaczenie ta kategoria usterek ma w przypadku nośników półprzewodnikowych, odpowiadając za niemal wszystkie ich uszkodzenia [<https://kaleron.pl/awarie-SSD.php>] oraz w dyskach SMR.

Najbardziej typowe objawy usterek oprogramowania układowego, to:

- zawieszanie urządzenia (brak odpowiedzi na polecenia, brak wymiany danych, ustawiony bit BSY w rejestrze stanu, zawieszanie komputera na 20–30 sekund przy próbie uruchomienia z podłączeniem uszkodzonego nośnika),
- detekcja z nieprawidłowym modelem (tzw. paszport technologiczny, zamiast nazwy modelu określonej przez producenta nośnika pojawia się nazwa typowa dla danego kontrolera, np.

SATAFIRM S11 dla SSD na kontrolerze PS-3111, czasem w paszporcie technologicznym pojawiają się też komunikaty diagnostyczne – tak np. numery seryjne w SSDkach na kontrolerach Intela były zastępowane kodami błędów),

- detekcja z zerową lub bardzo niską (kilka – kilkadziesiąt MB) pojemnością,
- w niektórych przypadkach dysk przechodzi inicjalizację poprawnie i wychodzi w gotowość przedstawiając się poprawną pojemnością, ale wszystkie sektory LBA czytają się jako puste lub z błędami.

W przypadku dysków twardych, sprawiają one wrażenie, jakby pracowały normalnie, proces inicjalizacji przechodzi poprawnie aż do odnalezienia strefy serwisowej i zatrzymuje się dopiero na obsłudze błędów przy jej odczycie (zawieszenie) lub przechodzi do końca, jednak nie pozwalając na dostęp do adresacji LBA (wyjście w gotowość bez możliwości odczytu danych). Głowice nie stukają, z rzadkimi wyjątkami dysków SMR firmy WD, gdzie przy uszkodzeniach translatora drugiego poziomu mogą pojawić się chwilowe odgłosy przypominające problemy z odczytem sygnału serwo i gubieniem ścieżki. W dyskach Seagate pokolenia F3 błędna detekcja z pojemnością 4 GB, zazwyczaj poprzedzona kilkusekundowym stukiem głowic i zatrzymaniem silnika oznacza uszkodzenie mechaniczne wymagające wymiany bloku magnetycznych głowic. Podejmowanie w takim dysku prób naprawy oprogramowania układowego bez uprzedniej wymiany głowic grozi pogorszeniem jego stanu.

Dyski SSD zazwyczaj zawieszają się lub przedstawiają się w charakterystyczny dla danego kontrolera sposób. Kontroler wydziela ciepło zbliżone do ciepła wydzielanego przez kontrolery tego typu w sprawnych urządzeniach. Dyski SSD z uszkodzeniami oprogramowania układowego na ogół wychodzą w gotowość i pozwalają na komunikację w ograniczonym zakresie po wprowadzeniu ich w tzw. tryb serwisowy (technologiczny) – *Safe Mode*. Zazwyczaj robi się to zwierając odpowiednie punkty kontrolne na PCB.

Półprzewodnikowe nośniki przenośne zazwyczaj są detektowane przez system operacyjny. Pojawia się komunikat o ich wykryciu, ale z zerową pojemnością. Często też pojawia się komunikat o braku nośnika w urządzeniu. Programy diagnostyczne zazwyczaj poprawnie rozpoznają model kontrolera (czasem tylko jego identyfikator), a często także identyfikator pamięci.

Problemy oprogramowania układowego w teorii zawsze są możliwe do rozwiązania, jednak w praktyce często sprawiają poważne trudności. Prócz kwestii unikatowości modułów najczęściej ulegających uszkodzeniom, częstym problemem, zwłaszcza w nowszych nośnikach jest zabezpieczenie oprogramowania układowego przed ingerencjami z zewnątrz oraz szyfrowanie. Inną przeszkodą może być fizyczna degradacja nośnika utrudniająca zapisanie na nim poprawionych modułów.

Uszkodzenia oprogramowania układowego rzadko dotyczą kodu wykonywalnego, a najczęściej polegają na błędnych zapisach w różnego rodzaju logach lub tablicach parametrycznych niezbędnych dla poprawnej pracy dysku. Takie uszkodzenia mogą wynikać z błędów i przekłamań przy zapisie zmian, gwałtownego zaniku zasilania podczas zapisu, fizycznej degradacji nośnika w obszarach przeznaczonych na przechowywanie informacji serwisowej lub przepełnienia obszaru przeznaczonego na rejestrację określonej informacji. Kluczowym problemem w naprawie usterek oprogramowania układowego jest to, że zazwyczaj dotyczą one informacji unikatowej dla danego egzemplarza nośnika, jakiej nie można zastąpić informacją pochodzącą z innego urządzenia.

Błędy oprogramowania układowego najczęściej dotyczą podsystemu translacji adresów LBA na fizyczne, co ma krytyczne znaczenie dla dostępu do danych użytkownika. Z tego względu, przed próbą naprawy błędów tego typu konieczne należy zabezpieczyć stan wyjściowy i zachować szczególną ostrożność, by nie doprowadzić do pogorszenia sytuacji. W szczególności utrata choćby i uszkodzonych oryginalnych fragmentów oprogramowania układowego i zastąpienie ich inną zawartością może mieć krytyczne znaczenie dla dalszego procesu odzyskiwania danych.

W dyskach SMR i SSD w niektórych przypadkach uszkodzenia translatora objawiają się tym, że dysk jest detektowany poprawnie, z prawidłowym modelem i pełną pojemnością, ale wszystkie sektory są wyzerowane. Taki objaw w większości wypadków wskazuje na zniszczenie danych przez ich nadpisanie, jednak istnieje inna możliwość. Przez błędy w translatorze dysk nie odczytuje fizycznie zawartości, a po prostu w odpowiedzi na polecenie odczytania dowolnego sektora zwraca zera.

W takiej sytuacji warto zweryfikować, czy można odczytać jakąś zawartość w adresacji fizycznej. Zejście do adresacji fizycznej może pozwolić na przynajmniej częściowe odzyskanie danych także w przypadku nieprawidłowej implementacji procedury *Secure Erase*. W niektórych przypadkach operacja *Secure Erase* sprowadza się do naniesienia odpowiedniej informacji w tablicach translatora bez fizycznego zniszczenia danych [Fukami 2024].

Inne popularne błędy dotyczą przepełniania logów SMART (*Self-Monitoring, Analysis and Reporting Technology*) i list sektorów niestabilnych. Ponieważ w tych przypadkach nie jest to informacja krytyczna dla uruchomienia nośnika i dostępu do danych, rozwiązaniem problemu może być wyczyszczenie przepełnionych modułów. Rzadziej zdarzają się uszkodzenia fragmentów oprogramowania, jakie mogą być po prostu skopiowane od nośnika z tą samą wersją oprogramowania układowego lub modułów konfiguracyjnych, jakie mogą być skopiowane i wykorzystane po niewielkich i relatywnie prostych poprawkach.

Do kategorii problemów oprogramowania układowego często zalicza się też ograniczenie pojemności nośnika przy pomocy funkcji HPA (*Host Protected Area*) lub DCO (*Device Configuration Overlay*). Często to ograniczenie nie jest usterką w ścisłym sensie, a jest wykorzystywane świadomie w celach serwisowych, eksploatacyjnych lub dla ukrycia danych [Gupta, Hoeschele, Rogers 2006]. Jednak czasami takie ograniczenie pojemności może pojawić się samoistnie, w wyniku błędów oprogramowania. Popularnym do niedawna przykładem takiej usterki było ograniczenie pojemności dysków 1 TB do 32 MB (0xFFFF sektorów) przez BIOSy (*Basic Input/Output System*) płyt głównych firmy Gigabyte.

Z uwagi na różnorodność występujących usterek, architektur oprogramowania układowego oraz różnice występujące pomiędzy poszczególnymi rodzinami modeli i wersjami oprogramowania układowego, usterki te zawsze wymagają dokładnej diagnostyki i zrozumienia problemu przed podjęciem próby jego rozwiązania. W szczególności ryzykowne jest pochopne przeklikywanie zautomatyzowanych procedur udostępnianych przez zaawansowane oprogramowanie do odzyskiwania danych. Takie procedury zostały opracowane z myślą o najpopularniejszych problemach, co zapewnia im dosyć wysoką skuteczność, jednak nie daje żadnej gwarancji, że konkretny problem mieści się w kategorii najbardziej popularnych.

W przypadku dysków twardych dobrą praktyką jest zabezpieczenie wszystkich dostępnych kopii zawartości strefy serwisowej. Często odbudowa uszkodzonych modułów jest możliwa

przez złożenie ich w całość z poprawnie odczytanych sektorów uszkodzonych kopii. Czasem konieczne jest wykorzystanie zależności, np. pomiędzy translatorem, a listami defektów. W skrajnych przypadkach brakujące fragmenty można próbować uzupełniać manualnie.

W razie braku możliwości zapisania poprawionych modułów w strefie serwisowej, można próbować przeprowadzić częściową inicjalizację dysku i załadować poprawione moduły do bufora RAM (*Random Access Memory*) z pliku. W niektórych dyskach można przeprowadzić procedurę *Hot-Swap*. Polega ona na zapisaniu poprawionej zawartości strefy serwisowej do innego, dostatecznie podobnego dysku. Następnie uruchamia się ten dysk, usypia i przy podłączonym zasilaniu przenosi PCB z w pełni załadowanym do bufora RAM oprogramowaniem układowym do pacjenta.

Dla nośników półprzewodnikowych istnieją liczne narzędzia do ich naprawy w przypadku uszkodzeń oprogramowania układowego [<https://www.usbdev.ru>, <https://flashboot.ru>]. Niestety wciąż jeszcze można się spotkać z przekonaniem, że najlepszą drogą do odzyskania danych jest naprawa urządzenia. Zasada działania tych programów polega na inicjalizacji pamięci Flash-NAND, skasowaniu wszystkich fizycznych bloków, przeskanowaniu ich pod kątem występujących defektów i utworzeniu nowych tablic warstwy translacji Flash. Procedura ta bezpowrotnie niszczy dane, a także, z uwagi na fizyczną degradację układów pamięci, nie może zagwarantować długotrwałego działania nośnika po naprawie.

Jeszcze niedawno bardzo popularną metodą odzyskiwania danych z nośników półprzewodnikowych było wylutowywanie układów Flash-NAND, odczytywanie ich na programatorze, a następnie dekodowanie pozyskanych w ten sposób obrazów binarnych i składanie ich w obraz struktury logicznej [Šestanjanj 2016]. Metoda ta sprowadzała się do odtworzenia i emulacji operacji wykonywanych przez kontroler nośnika. Jednak wraz z rosnącą złożonością matematyczną wykorzystywanych algorytmów i upowszechnieniem szyfrowania, metoda ta zaczęła tracić na znaczeniu. W szczególności szyfrowanie w praktyce uniemożliwia jej sensowne wykorzystanie.

Drugie, coraz popularniejsze podejście polega na wprowadzeniu nośnika w tryb serwisowy i załadowaniu do jego pamięci operacyjnej odpowiednio przygotowanego programu – *loadera*. Uruchomiony w ten sposób nośnik pozwala na wykonywanie poleceń technologicznych, które pozwalają na odbudowę oprogramowania układowego, w tym podsystemu translacji, i uzyskanie dostępu do danych. Głównym problemem tej metody jest jej złożoność i konieczność przeprowadzenia badań w zakresie inżynierii wstecznej osobno dla każdego kontrolera, a typowo i dla każdej wersji oprogramowania układowego.

Z tego powodu zastosowanie tej metody w praktyce najczęściej jest ograniczone do wykorzystywania *loaderów* udostępnianych w komercyjnych narzędziach. Niezbędny dla opracowania odpowiedniego narzędzia nakład pracy, czas i uwarunkowania ekonomiczne sprawiają, że obsługiwana w ten sposób jest jedynie niewielka grupa najpopularniejszych kontrolerów. Dodatkowym problemem są postępy w zabezpieczaniu nośników przed przełamaniem szyfrowania, przez co nowsze modele są odporniejsze na znane metody ataków.

Ze względu na niewielką liczbę ośrodków zajmujących się poważnymi badaniami nośników danych w zakresie ich usterek i możliwości odzyskiwania danych, postępy w tej dziedzinie nie nadążają za rosnącą liczbą i złożonością występujących problemów. Biorąc pod uwagę to, w jaki sposób rosnąca gęstość zapisu wymusza wprowadzenie kolejnych, coraz bardziej złożonych rozwiązań w zakresie korekcji błędów, zarządzania defektami, adresacji danych oraz optymalizacji

pracy nośników, bez istotnego zwiększenia zaangażowania w badanie tych zagadnień, dystans pomiędzy tym, co jest fizycznie możliwe, a tym, co jest praktycznie wykonalne będzie się tylko powiększał. Z tego względu możemy coraz częściej spotykać się z sytuacjami, kiedy z praktycznych powodów dane fizycznie możliwe do odzyskania nie zostaną odzyskane.

3.4. Degradacja nośnika danych

Częstą przyczyną uszkodzeń nośników danych jest ich degradacja. W takich przypadkach nośnik poprawnie przechodzi inicjalizację, wychodzi w gotowość i umożliwia dostęp do adresacji LBA. Jednak podczas prób odczytu zawartości pojawiają się problemy, jak bardzo wolny odczyt, uszkodzone pliki, częste uruchamianie narzędzi do sprawdzania spójności systemów plików, jak *chkdsk*, *scandisk* lub *fsck*, uszkodzone sektory, ostrzegawcze komunikaty podsystemu SMART [Kaczmarzyk 2024e], a w przypadku dysków twardych – także głośna praca i nietypowe dźwięki pracy głowic.

Degradację stanu nośnika można zweryfikować przy pomocy skanu programami diagnostycznymi. Programy te sprawdzają czasy dostępu do poszczególnych sektorów LBA niezależnie od ich zawartości i zaadresowania w strukturach logicznych systemów plików. W przypadku wykrycia błędów, dobre programy diagnostyczne zwrócą informację o rodzaju błędu pobraną z rejestru błędów [Kaczmarzyk 2024d].

W czasie diagnostyki warto zwrócić uwagę na rodzaj problemów z odczytem, gdyż czasami nośnik faktycznie nie jest zdegradowany, a przyczyna problemów z odczytem leży gdzie indziej. Np. błędy typu ABRT (odmowa wykonania polecenia) często są związane z zabezpieczeniem dysku hasłem ATA. Czasem też bardzo duża liczba błędów odczytu przy jednoczesnej szybkiej i cichej pracy dysku może wynikać z problemów translatora. W przypadku dysków Seagate w takiej sytuacji występują błędy typu UNC (błąd sumy kontrolnej), a w przypadku WD – IDNF (nieprawidłowy identyfikator sektora).

W dyskach SSD algorytmy zarządzania defektami zazwyczaj skutecznie eliminują uszkodzone bloki z eksploatacji i takie bloki rzadko można wykryć skanowaniem. Ich ujawnienie w czasie skanu zazwyczaj oznacza, że stan SSDka jest już katastrofalny. Podczas diagnostyki SSDków warto zwrócić uwagę na czasy odczytu. Niestabilność i bardzo wolny odczyt zwykle wskazuje na wysoki stopień zużycia układów pamięci [Kaczmarzyk 2024b].

Ze względu na ryzyko pogorszenia stanu zdegradowanych nośników, w czasie diagnostyki należy zwracać uwagę, aby nie obciążać nadmiernie nośnika. W większości przypadków dla odzyskania danych nie jest potrzebna pełna wiedza na temat stanu powierzchni nośnika i nie ma potrzeby ponoszenia ryzyka pogłębienia usterki dla zdobycia tej wiedzy. Ponieważ skan polega na odczytywaniu kolejnych sektorów, warto, po ogólnym zorientowaniu się w stanie dysku, jak najszybciej przystąpić do wykonania kopii posektorowej. Warto przy tym pamiętać, że kopię posektorową można wykonywać też fragmentami i w przypadku napotkania bardziej zdegradowanych obszarów można je pominąć, by najpierw zabezpieczyć zawartość sektorów łatwiejszych do skopiowania, a do trudniejszych wrócić później.

Zasadniczo dane zapisane w uszkodzonych obszarach są niemożliwe do odzyskania, ale nie wszystko jest tak jednoznaczne. Przy współcześnie osiąganym gęstości zapisu jest praktycznie niemożliwe zapisywanie i odczytywanie danych bez błędów. Dlatego każda fizyczna jednostka

alokacji w każdym nośniku jest zabezpieczona kodami korekcji błędów (ECC). Kody te pozwalają korygować występujące błędy i odczytywać poprawną zawartość, jednak ich możliwości korekcyjne są ograniczone [Riggle, McCarthy 1998, Sweeney 2002]. I z błędem odczytu mamy do czynienia w sytuacji, kiedy liczba błędów bitowych przekracza możliwości korekcyjne zastosowanego kodu.

Przy tym liczba bitowych błędów w niektórych wypadkach jedynie nieznacznie przekracza możliwości korekcyjne kodu. To otwiera możliwości podjęcia kolejnych prób doczytania sektorów, które w pierwszym podejściu okazały się nieczytelne. Przy tym trzeba pamiętać, że wpływ na błędy odczytu może mieć wiele czynników, jak stabilność napięć zasilania lub fluktuacje termiczne i kontrola tych czynników może wpływać na poprawę wyników odczytu.

W szczególności na poprawę jakości odczytu układów pamięci Flash-NAND może wpływać kontrola temperatury, w jakiej przeprowadzany jest odczyt [Pawlikowski 2024]. Warto też przetestować możliwości wykorzystania obniżonych lub podwyższonych w stosunku do nominalnych napięć zasilających. Natomiast w przypadku dysków twardych niekiedy pomaga zmiana położenia dysku w czasie odczytu.

Nie ma jednej metody postępowania w takich sytuacjach. Dla każdego przypadku środki poprawy jakości odczytu należy dobierać eksperymentalnie, obserwując rezultaty. Przy tym należy unikać gwałtownych zmian, aby minimalizować ryzyko pogłębienia degradacji lub spowodowania poważniejszych uszkodzeń nośnika.

3.5. Uszkodzenia struktur logicznych

Z uszkodzeniami logicznymi mamy do czynienia w sytuacjach, kiedy nośnik, jako urządzenie techniczne, jest sprawny, ale błędy w strukturach logicznych nie pozwalają na uzyskanie dostępu do danych lub kiedy błędy w strukturach logicznych wynikają z uszkodzeń nośnika, np. jego degradacji. Zwłaszcza w drugim, ze wskazanych wyżej przypadków, problemy logiczne najlepiej rozwiązywać pracując na wykonanej wcześniej kopii, aby ograniczyć obciążenie oryginalnego nośnika i ryzyko pogorszenia jego stanu. Uszkodzenia logiczne mogą obejmować tablice partycji, metadane systemów plików [Kaczmarzyk 2023b] lub też błędy w samych plikach.

Ogólnie zawartości utraconej czy to w wyniku błędów odczytu, czy to zastąpienia inną treścią (nadpisanie [Kaczmarzyk 2023c]) nie da się odzyskać. Jednak często odtworzenie i naprawa struktur logicznych jest możliwa z wykorzystaniem kopii metadanych oraz matematycznych zależności pomiędzy poszczególnymi parametrami. Wiele takich problemów mogą automatycznie naprawić programy do odzyskiwania danych, inne trzeba rozwiązywać manualnie.

Fakt, że nawet zaawansowane narzędzia nie potrafią odnaleźć pewnych śladów, zwracają niekompletne wyniki lub odzyskują uszkodzone pliki, nie oznacza, że to, czego nie udało się odnaleźć automatycznymi środkami, faktycznie nie istnieje. Istotnym ograniczeniem oprogramowania do odzyskiwania danych i informatyki śledczej jest to, że przy identyfikacji obiektów bazują one na predefiniowanych sygnaturach i nawet niewielka niezgodność (np. błąd bitowy) może spowodować nieuwzględnienie w rezultatach czegoś, na co można łatwo zwrócić uwagę przeglądając zawartość nośnika w edytorze szesnastkowym. Ponadto zautomatyzowane narzędzia bardzo słabo sobie radzą z plikami pofragmentowanymi.

Istotną przeszkodą w uzyskaniu dostępu do danych często jest szyfrowanie zawartości nośnika. Prócz wspomnianego wcześniej szyfrowania na poziomie sprzętowym, typowo obejmującego cały dysk (FDE – *Full Disc Encryption*), możemy spotkać szyfrowanie na poziomie

partycji (FVE – *Full Volume Partition*) lub plików (FBE – *File Based Encryption*). Ponadto dane na dysku mogą być ukryte w postaci zaszyfrowanych kontenerów, które niekoniecznie muszą być widoczne w strukturze logicznej (np. *TrueCrypt* lub *VeraCrypt*).

Z uwagi na to, że dane zaszyfrowane nie odpowiadają predefiniowanym sygnaturom, narzędzia do odzyskiwania danych i informatyki śledczej nie są w stanie odnaleźć w zaszyfrowanym strumieniu danych żadnej sensownej zawartości. Fakt zaszyfrowania nośnika lub jego części można z bardzo dużym prawdopodobieństwem ustalić na podstawie łatwego do zauważenia w edytorze szesnastkowym wypełnienia go strumieniem danych o wysokiej entropii. Dane zaszyfrowane w teorii są w pełni odzyskiwalne, jednak praktycznym warunkiem dla ich odszyfrowania jest konieczność posiadania klucza szyfrującego.

Najczęściej kompromitacja systemu szyfrującego odbywa się poprzez odnalezienie miejsca przechowywania klucza szyfrującego lub odkrycie sposobu pozwalającego na nieautoryzowane wymuszenie jego użycia. Z uwagi na długość i wysoką entropię kluczy szyfrujących, ataki typu *Brutforce* bezpośrednio na klucz nie rokują na osiągnięcie rezultatu w sensownym czasie i nie mają praktycznego znaczenia. Natomiast celowe mogą być ataki na piny i hasła zabezpieczające dostęp do klucza. Tego typu zabezpieczenia zazwyczaj są krótsze i prostsze, przy tym często podatne na ataki słownikowe.

Poważnym ograniczeniem manualnych analiz jest ich czaso- i pracochłonność, co przy współczesnych pojemnościach nośników praktycznie wyklucza możliwość ich dokładnej analizy w warunkach ograniczeń czasowych i budżetowych. Dlatego nie można sobie wyobrazić efektywnej pracy specjalisty bez wykorzystania odpowiednich narzędzi. Tym niemniej praca ta nie powinna się ograniczać do przeprowadzenia skanowania i automatycznego wygenerowania raportu, a powinna być uzupełniona weryfikacją i pogłębioną analizą wyników. Z tego względu specjaliści odzyskiwania danych i informatyki śledczej powinni mieć odpowiednie kompetencje w zakresie znajomości struktur logicznych systemów plików i praktycznego posługiwania się edytorem szesnastkowym.

4. Najważniejsze zasady zabezpieczenia nośników danych i ich zawartości

4.1. Podstawy zabezpieczania nośników informacji i odzyskiwania danych

Przystępując do zabezpieczenia cyfrowych dowodów trudno z góry przewidzieć wszystkie problemy, jakie przyjdzie rozwiązać w celu uzyskania dostępu do danych. Dlatego należy postępować z ostrożnością, minimalizować ryzyko błędów, unikać nadmiernych ingerencji i nie podejmować nieuzasadnionych działań. Warto przy tym w dążeniu do jak najszybszego zabezpieczenia jak największej części dostępnej informacji nie zapominać o ryzyku niepowodzenia i pogorszenia stanu nośnika i w związku z tym unikać ingerencji zamykających drogę do zastosowania innych środków.

Do pracy z nośnikami najlepiej przystępować na przygotowanym stanowisku pracy, dysponując wszystkimi potrzebnymi narzędziami oraz komputerem z zainstalowanym niezbędnym oprogramowaniem. Na komputerze używanym do odzyskiwania danych należy wyłączyć obsługę funkcji TRIM. Dyski najlepiej podłączać za pośrednictwem sprzętowych blokerów zapisu lub specjalistycznych kontrolerów do odzyskiwania danych. Należy bezwzględnie chronić je przed

nadpisaniem, czy to przypadkowym, czy intencjonalnym (np. inicjalizacja dysku w odpowiedzi na propozycję systemu operacyjnego).

Pracę na improwizowanych stanowiskach i w warunkach polowych należy traktować jako ostateczność i podejmować ją jedynie w wyjątkowych sytuacjach. Podobnie należy unikać prób zdalnego odzyskiwania danych. Prócz tego, że ze względów bezpieczeństwa wskazane jest, aby komputery używane do odzyskiwania danych były odseparowane od sieci, w procesie odzyskiwania danych duże znaczenie mają czynniki, które trudno obserwować zdalnie, np. odgłosy pracy dysku twardego, czy temperatura nośnika.

Zasadniczo w procesie odzyskiwania danych można wyróżnić następujące etapy [Сенкевич 2011]:

- diagnostyka,
- uzyskanie dostępu do nośnika,
- wykonanie obrazu nośnika,
- rekonstrukcja struktury logicznej,
- odzyskanie plików,
- pozyskanie informacji zawartej w plikach.

Przebieg poszczególnych etapów i niezbędnych czynności w konkretnym przypadku jest determinowany charakterem usterki. Należy przy tym pamiętać, że pewne czynności i ingerencje uzasadnione z technicznego punktu widzenia mogą być niedopuszczalne ze względów proceduralnych i mogą prowadzić do formalnego podważenia nieprawidłowo zabezpieczonych dowodów. Z tego samego powodu konieczne jest też odpowiednie dokumentowanie podejmowanych czynności.

4.2. Diagnostyka

Przystępując do diagnostyki nośników warto zebrać jak najbardziej szczegółowe informacje na temat urządzenia, jego stanu i zawartości oraz ewentualnych okoliczności powstania uszkodzeń. Trzeba przy tym pamiętać, że wiarygodność takich informacji jest ograniczona. Po pierwsze osoby przekazujące nośnik do analizy lub osoby, u których ten nośnik jest zabezpieczany niekoniecznie muszą dysponować odpowiednią wiedzą na temat urządzenia lub kompetencjami pozwalającymi dostatecznie szczegółowo i precyzyjnie opisać jego stan. Po drugie – mogą być zainteresowane celowym wprowadzeniem organów ścigania i wymiaru sprawiedliwości oraz analityków w błąd.

Przy zabezpieczeniu nośników danych najważniejsze jest, by nie dopuścić do pogorszenia ich stanu. Należy mieć na uwadze, że mogły być wobec nich podejmowanie działania mające na celu uniemożliwienie dostępu do informacji. Przed przystąpieniem do jakichkolwiek czynności, należy uważnie obejrzeć nośniki pod kątem uszkodzeń mechanicznych, termicznych lub elektrycznych, śladów zalania i korozji oraz innych możliwych ingerencji.

Także podczas transportu i przechowywania należy chronić nośniki przed możliwością uszkodzeń wtórnych. Trzeba przy tym pamiętać, że szereg urządzeń, zwłaszcza mobilnych może wciąż komunikować się drogą bezprzewodową, w tym otrzymywać i wykonywać polecenia mające na celu usunięcie z nich zawartości lub ich zablokowania. Z tego względu, w przypadku takich urządzeń konieczne jest fizyczne uniemożliwienie im komunikacji ze światem zewnętrznym [Kaczorowski i in. 2026].

W przypadku zauważenia uszkodzeń, należy je usunąć przed uruchomieniem nośnika. Nie należy też uruchamiać nośników ze śladami zalania, korozji i oddziaływania termicznego, a w przypadku dysków twardych – także w przypadku podejrzeń otwierania hermobloku, bez uprzedniego szczegółowego sprawdzenia jego stanu. W przypadku dysków twardych szczególnie niebezpieczne jest ich uruchomienie z jakimikolwiek zanieczyszczeniami wewnątrz hermobloku, brakującymi lub nadmiarowymi elementami, wygiętymi ślizgaczami lub urwanymi głowicami, które mogą doprowadzić do zniszczenia magnetycznych powierzchni talerzy.

Diagnostyka nośników danych jest zbyt obszernym zagadnieniem, by mogła tu zostać szczegółowo opisana. Przy jej przeprowadzaniu należy opierać się na znajomości budowy i zasad funkcjonowania urządzeń oraz ich procedury startowej [Kaczmarzyk 2023a]. Warto też zwracać uwagę na opisane we wcześniejszej części najbardziej typowe objawy poszczególnych usterek. Należy przy tym podchodzić do diagnostyki z ostrożnością i dokładnością, unikając rutynowego podejścia i z góry przyjmowanych założeń, nawet, jeśli statystycznie takie założenia często się sprawdzają.

4.3. Uzyskanie dostępu do zawartości nośnika

Uzyskanie dostępu do zawartości nośnika często wymaga usunięcia usterek stwierdzonych podczas diagnostyki. W wielu przypadkach konieczna jest wymiana uszkodzonych elementów elektronicznych lub całych podzespołów, jak np. blok magnetycznych głowic. W innych sytuacjach niezbędne są ingerencje w oprogramowanie układowe, w tym usunięcie lub przełamanie zabezpieczeń. W przypadku ingerencji w oprogramowanie układowe, trzeba pamiętać o zabezpieczeniu stanu wyjściowego, aby mieć możliwość powrotu, gdyby wprowadzone zmiany nie przyniosły pożądanego rezultatu.

W przypadku uszkodzonych nośników półprzewodnikowych istnieją dwa zasadnicze podejścia do pozyskania ich zawartości. Praca w tzw. trybie serwisowym (technologicznym – *safe mode*) i odczyt na programatorze zawartości wylutowanych układów pamięci. Warto w tym miejscu przypomnieć, że w przypadku nośników szyfrowanych to drugie podejście jest bezcelowe, a w innych sytuacjach pierwsze zazwyczaj jest łatwiejsze, mniej pracochłonne i przynoszące lepsze rezultaty. Z tego względu typowo pierwszeństwo należy dać próbom uzyskania z nośnikiem względnie stabilnej komunikacji, a dopiero w dalszej kolejności rozważyć jego rozlutowanie. Przy lutowaniu układów pamięci należy zwrócić uwagę na to, by ich nie przegrzewać ani nie doprowadzić do uszkodzenia wyprowadzeń.

Jeżeli mamy do czynienia ze sprawnym dyskiem SSD, z którego zostały usunięte dane, taki dysk również należy wprowadzić w tryb serwisowy. Wszystkie współczesne dyski SSD obsługują funkcję TRIM, która sprawia, że skasowane pliki momentalnie przestają być widoczne w adresacji LBA i rozpoczyna się proces ich fizycznego kasowania. Proces ten jest przeprowadzany przez oprogramowanie układowe dysku niezależnie od innych poleceń otrzymywanych z zewnątrz i nawet podłączenie dysku przez sprzętowy bloker zapisu nie może już powstrzymać fizycznego kasowania bloków. Kasowanie bloków można zatrzymać wprowadzając dysk w tryb serwisowy i zajmując kontroler poleceniami odczytu poszukiwanych danych w adresacji fizycznej.

4.4. Wykonanie obrazu nośnika

Wykonanie obrazu (sklonowanie) nośnika można wykonać do innego dysku lub do pliku binarnego. Każdy z tych wariantów ma swoje zalety i swoje ograniczenia i trudno jednoznacznie wskazać, który z nich jest lepszy. Wyboru, gdzie będzie klonowany obraz dysku, dokonuje się w oparciu o specyfikę zadania, obowiązujące wewnętrzne procedury, dostępną infrastrukturę oraz osobiste preferencje operatora.

Kiedyś typowym sposobem postępowania było wykonywanie kopii binarnej nośnika, jako całości, ale upowszechnienie szyfrowania wymusiło zmianę tego podejścia. Wykonanie obrazu zaszyfrowanego i nienadającego się do sensownej analizy nośnika mija się z celem. Dlatego obecnie w przypadkach nośników zaszyfrowanych dąży się do odblokowania urządzenia, przełamania szyfrowania i pozyskania obrazu odszyfrowanych partycji, a nie surowego obrazu zaszyfrowanej zawartości nośnika.

Środki i narzędzia niezbędne dla wykonania obrazu nośnika w dużym stopniu zależą od jego stanu technicznego. W przypadku nośników sprawnych w zupełności wystarczające jest linuksowe polecenie `dd` lub proste, popularne, darmowe oprogramowanie do klonowania dysków [Nikkel 2021]. W informatyce śledczej popularne są różnego rodzaju duplikatory pozwalające m.in. na klonowanie urządzeń ze zdegradowaną powierzchnią i zapewniające odpowiednią obsługę błędów odczytu, jednocześnie pełniąc funkcję blokera zapisu na dysk źródłowy.

Dla najbardziej skomplikowanych i niestabilnych przypadków, w tym części dysków po wymianie głowic, wskazane jest użycie specjalistycznych kontrolerów współpracujących z oprogramowaniem do odzyskiwania danych. Tego typu kontrolerów używa się także w wielu przypadkach uszkodzeń oprogramowania układowego. Oprogramowanie do obsługi takich kontrolerów pozwala na szeroki zakres ingerencji, w tym zmiany zawartości bufora RAM dysku, ładowanie do niego odpowiednio przygotowanej zawartości z pliku, czy zbudowanie wirtualnego translatora.

W przypadku odzyskiwania danych z wylutowanych układów Flash-NAND niezbędne jest ich zdekodowanie, skorygowanie zawartości przy pomocy kodów ECC i odseparowanie danych użytkownika od informacji nadmiarowej. Następnie należy fizyczne jednostki alokacji złożyć w logicznej kolejności w celu uzyskania spójnego obrazu struktury logicznej. W teorii zadanie to jest wykonalne z pomocą dowolnego edytora szesnastkowego, jednak jego złożoność sprawia, że do efektywnej pracy wykorzystuje się wyspecjalizowane oprogramowanie.

O ile w przypadku dysków sprawnych wykonanie obrazu nie nastrocza trudności i nie jest obarczone ryzykiem, w przypadku urządzeń uszkodzonych należy brać pod uwagę możliwość pogorszenia ich stanu i dostosować podejście do ich klonowania do specyfiki zadania. W szczególności można dążyć do wyklonowania jak największej objętości zawartości omijając najbardziej problematyczne obszary i wracając do nich później. Warto pamiętać, że klonowanie można wykonywać fragmentami i decyzję o wyborze kolejnych fragmentów można podejmować na podstawie analizy danych wyklonowanych wcześniej. Należy przy tym unikać obciążenia dysku powtórным klonowaniem obszarów już sklonowanych.

W szczególności w pierwszej kolejności warto wyklonować obszary metadanych systemów plików i zdecydować o klonowaniu najpierw wybranych partycji, potencjalnie zawierających najbardziej interesujący materiał, a dopiero później partycji o potencjalnie mniej istotnej zawartości. Można przy tym w zależności od potrzeb i specyfiki zadania skupić się na klonowaniu najpierw zajętego (zaalokowanego w strukturach logicznych) lub wolnego miejsca albo od razu

przystąpić do wyszukiwania szczególnie istotnych plików, np. baz danych. W przypadku wykonywania obrazu do plików binarnych, wyklonowane w ten sposób fragmenty należy potem złożyć w całość.

Przy wykonywaniu kopii posektorowej warto zwrócić uwagę na obszary, w jakich mogły być ukrywane dane. Mogą to być np. obszary pomiędzy początkiem dysku, a pierwszą partycją, pod koniec dysku lub odstępy między partycjami. Zdarza się też, że dane ukrywane są w końcowych obszarach dysku, które później są wyłączane z adresacji LBA za pomocą funkcji HPA lub DCO i przestają być widoczne dla systemów operacyjnych i większości programów.

Po wykonaniu obrazu warto wykonać jego dodatkową kopię, aby dalsze czynności wykonywać na kopii obrazu. Pozwala to uniknąć powtarzania procesu klonowania w przypadku wystąpienia awarii lub błędu ludzkiego. Po zakończeniu klonowania (wykonaniu pełnej kopii nośnika, sklonowaniu wszystkiego, co jest technicznie możliwe lub zakończeniu procesu w przypadku stwierdzenia niecelowości jego kontynuacji) zwykle wylicza się dla pozyskanego obrazu funkcję skrótu. Szeroko stosuje się także rejestrowanie znaczników czasowych wykonywania obrazu.

4.5. Rekonstrukcja struktury logicznej

W pierwszym podejściu do rekonstrukcji struktury logicznej zazwyczaj wykorzystuje się zautomatyzowane procedury programu do odzyskiwania danych. Programy tego typu potrafią przeanalizować znalezione fragmenty metadanych systemów plików i wykorzystać je do odbudowy struktur logicznych oraz wirtualnego uzupełnienia brakujących elementów i wartości np. na podstawie kopii danej struktury lub znanych wzajemnych powiązań pomiędzy pewnymi strukturami. Z uwagi na to, że struktury logiczne poszczególnych systemów plików są dosyć dobrze znane, algorytmy sensownych programów do odzyskiwania danych są bardzo zbliżone i dają podobne rezultaty.

Słabością zautomatyzowanych algorytmów jest to, że na ogół nie potrafią one uzupełniać brakujących i poprawiać ewidentnie nieprawidłowych wartości parametrów ani podejmować złożonych decyzji w kategoriach prawdopodobieństwa w warunkach niepełnej informacji. W takich sytuacjach operator może podjąć próbę zbudowania wirtualnej partycji zadając programowi odpowiednie parametry w oparciu o własną wiedzę i doświadczenie lub osiągnąć pożądaný rezultat metodą prób i błędów. W pewnych sytuacjach uzasadnione są ingerencje w uszkodzone metadane systemu plików, które mogą wprost doprowadzić do naprawienia struktury logicznej lub umożliwić programom do odzyskiwania danych znalezienie lub uporządkowanie w strukturze katalogów większej liczby plików.

Z uwagi na procedury zabezpieczania dowodów cyfrowych, takie ingerencje mogłyby doprowadzić do formalnego podważenia dowodu. Dlatego powinno się ich dokonywać na dodatkowej kopii roboczej i na tej kopii prowadzić odpowiednie analizy, a dopiero dysponując ich wynikami, wrócić do analizy dowodu. Należy też wystrzegać się wyciągania naciąganych wniosków i dopasowywania wyników pod założoną tezę, np. dopasowywania na siłę znalezionych fragmentów metadanych zawierających nazwę i znaczniki czasowe do znalezionych plików.

Takie dopasowania oczywiście w pewnych sytuacjach mogą być uprawnione, jeśli przemawia za tym zgodność rozmiaru pliku i jego położenie w dostatecznym stopniu odpowiada

opisowi w metadanych. Dla pewnych typów plików można też porównać znaczniki czasu zawarte w ich wewnętrznych metadanych (np. Exif) ze znacznikami opisującymi ten plik w strukturach systemu plików, jednak trzeba pamiętać, że z wielu powodów te wartości mogą być rozbieżne [Baraniecki 2025a]. Przy tym należy mieć na uwadze, że takie działania jak najbardziej uzasadnione z technicznego punktu widzenia i praktykowane przy odzyskiwaniu danych, w sytuacji różnego rodzaju postępowań prawnych mogą być niedopuszczalne ze względów proceduralnych.

Innym popularnym, choć, z uwagi na ryzyko pogłębienia uszkodzeń metadanych, niezalecanym sposobem rekonstrukcji struktury logicznej systemu plików jest użycie narzędzi systemowych, jak *chkdsk*, *scandisk* lub *fsck*. Narzędzia te analizują metadane systemu plików, identyfikują błędy i je usuwają. Przy czym słowo „usuwać” należy rozumieć jak najbardziej dosłownie – uszkodzone fragmenty najczęściej są usuwane tak, żeby nie przeszkadzały w zamontowaniu partycji przez system operacyjny.

Usunięcie uszkodzonych fragmentów metadanych nie tylko może spowodować pogubienie, uszkodzenie lub bezpowrotną utratę większej liczby plików, ale też niszczy informację, jaka mogłaby być poddana analizie i posłużyć do wyciągnięcia wniosków pomagających w manualnej rekonstrukcji systemu plików. Ponadto procedury tego typu przeprowadzają niekontrolowane zapisy na dysku, które nie tylko stanowią niedopuszczalną ingerencję w jego zawartość, ale też są praktycznie nieodwracalne. Dlatego wykorzystanie tego typu procedur powinno być ograniczone tylko do sytuacji, kiedy mogą pomóc w zamontowaniu partycji i uruchomieniu systemu operacyjnego wymagającego „żywej” analizy i tylko pod warunkiem uprzedniego zabezpieczenia stanu wyjściowego. Trzeba też pamiętać o tym, by zabezpieczane nośniki chronić przed przypadkowym automatycznym uruchomieniem takich procedur.

4.6. Odzyskanie plików

W większości sytuacji rekonstrukcja struktury logicznej systemu plików pozwala na odzyskanie zaadresowanych w niej plików. Pod pewnymi, zależnymi od typu systemu plików i jego wewnętrznej architektury warunkami, często jest też możliwe odzyskanie części usuniętych plików w strukturze katalogów z ich oryginalnymi nazwami, znacznikami czasowymi i innymi obsługiwanymi przez dany system plików atrybutami (np. właścicielskimi). Jest to najbardziej pożądaný rezultat, jednak, z uwagi na usterki techniczne, błędy logiczne i celowo podejmowane działania kontrwykrywcze, nie zawsze możliwy do uzyskania. Przy tym to, że coś nie zostało odnalezione i zaadresowane w strukturze logicznej, jeszcze nie znaczy, że nie istnieje.

W przypadku, gdy uszkodzenia metadanych częściowo lub całkowicie uniemożliwiają odbudowę struktury logicznej systemów plików lub metadane usuniętych plików zostały zniszczone (np. węzły indeksowe w systemach plików wywodzących się ze środowiska uniksowego), zagubione pliki można próbować odnaleźć po sygnaturach (wyszukiwanie RAW). Nazwy odnalezionych w ten sposób plików różnią się od oryginalnych, utraconych nazw i są nadawane automatycznie przez programy do odzyskiwania danych. Typowo nazwy te opierają się o numer sektora, w jakim został odnaleziony nagłówek pliku, niekiedy mogą być uzupełnione pewnymi szczegółami w oparciu o wewnętrzne metadane pliku.

Wyszukiwanie RAW może zwrócić wiele wyników śmieciowych (przypadkowa zbieżność ciągu symboli z wzorcem sygnatury), plików uszkodzonych (np. pofragmentowanych lub częściowo nadpisanych inną zawartością) oraz duplikatów plików poprawnie zaadresowanych

w strukturze katalogów. W przypadku tych ostatnich, tworzony przez wyszukiwanie RAW bałagan można zmniejszyć ograniczając skanowanie do obszaru niezaalokowanego w systemie plików. Skanowanie obszaru niezaalokowanego w systemie plików może też przynieść ciekawe rezultaty w przypadku komputerów, na których niedawno doszło do przeinstalowania systemu operacyjnego. Oczywiście pod warunkiem, że dane nie zostały zniszczone przez nadpisanie lub w inny sposób, np. przez funkcję TRIM.

Ponadto nie każdy typ pliku ma sygnaturę pozwalającą na odnalezienie go przez wyszukiwanie RAW lub może mieć tę sygnaturę uszkodzoną. Z tego względu warto podjąć próbę odnalezienia potencjalnie interesujących ciągów symboli przy użyciu wyszukiwarki. Mogą to być np. dane osobowe lub kontaktowe figurantów albo słownictwo związane z charakterem prowadzonej sprawy. Odnaleźć w ten sposób można nie tylko pogubione pliki, ale też fragmenty plików dawno usuniętych i częściowo nadpisanych.

Przy użyciu wyszukiwarki warto pamiętać o różnych metodach kodowania danych i podejmować próby wyszukiwania zarówno z wykorzystaniem kodowania ASCII (*American Standard Code for Information Interchange*), jak i Unicode. W przypadku kodowania ASCII występują strony kodowe – różne zestawy znaków graficznych dla kodów z zakresu 0x80-FF, pozwalające m. in. na kodowanie tekstów w alfabetach niełacińskich. Zwłaszcza w przypadku przestępczości transgranicznej może się okazać, że wybór odpowiedniej strony kodowej pozwoli na odkrycie, że na pozór bezsensowny ciąg symboli w rzeczywistości jest obcojęzycznym tekstem.

4.7. Pozyskanie informacji zawartej w plikach

Pozyskanie informacji z odzyskanych plików, jeśli nie są one zaszyfrowane lub dostęp do nich nie został zabezpieczony hasłami, w przypadku plików sprawnych na ogół jest prostym zadaniem. Dla uzyskania dostępu do ich zawartości, wystarczy użyć odpowiedniego oprogramowania. Przy tym w przypadku niektórych kategorii urządzeń możemy mieć do czynienia ze specyficznymi formatami plików, metodami kodowania materiału audio i video (np. w różnego typu rejestratorach), a nawet specyficznych systemów plików (elektronika motoryzacyjna, urządzenia internetu rzeczy, drony). W takich przypadkach najlepiej mieć odpowiednie oprogramowanie od producenta urządzenia, a w jego braku, konieczna jest analiza w zakresie inżynierii wstecznej.

Innym problemem są uszkodzenia plików wynikające z fizycznych błędów odczytu lub częściowego nadpisania. W takich przypadkach sposób postępowania zależy od typu pliku. Dla części popularnych typów plików istnieją narzędzia do ich naprawy. Przy tym trzeba mieć na uwadze, że narzędzia te są w stanie naprawiać jedynie relatywnie niewielkie błędy i nie będą w stanie odtworzyć znacznych brakujących lub uszkodzonych fragmentów pliku.

Uszkodzone pliki audio i video często można odtwarzać, choć w miejscach uszkodzeń będą występowały zniekształcenia dźwięku i obrazu. Warto w takich wypadkach przetestować kilka różnych odtwarzaczy, gdyż, w zależności od zastosowanych algorytmów kodowania i kompresji, niektóre z nich mogą sobie radzić lepiej od innych. Szczególną przyczyną usterek plików video odzyskiwanych ze sformatowanych kart pamięci jest ich fragmentacja powodująca, że programy odzyskujące dane łączą nagłówki z niewłaściwymi plikami. Naprawa takich plików

jest możliwa przez odpowiednie połączenie nagłówków z właściwymi plikami przy pomocy edytora szesnastkowego [Kaczmarzyk 2025a].

W przypadku uszkodzonych plików niezaszyfrowanych i nieskompresowanych, jak znaczna część baz danych, pliki typu **.xml*, kod źródłowy oprogramowania, grafiki bitmapowe, czy starsze typy plików pakietów biurowych możliwe jest odczytanie znacznej części tekstu, wartości liczbowych, czy rekordów bazodanowych przy pomocy różnego rodzaju edytorów. Odzyskiwana w ten sposób zawartość nie będzie kompletna, ale może zawierać na tyle istotne informacje, że warto podjąć analizę tego typu. W przypadku baz danych brakujące rekordy często można uzupełnić z backupów lub starszych wersji plików często zapisywanych w podkatalogu typu „Archiwum” na tym samym dysku.

Specyficzną przyczyną uszkodzeń plików są ataki typu ransomware. Dla jak najszybszego uszkodzenia maksymalnej liczby plików, złośliwe oprogramowanie typowo poprzestaje na zaszyfrowaniu początkowego fragmentu pliku zawierającego jego nagłówek. W przypadku plików bazodanowych często możliwa jest naprawa pliku (zwykle z niewielkimi stratami) przez odtworzenie poprawnego nagłówka. Innym sposobem odszyfrowania zainfekowanych plików jest skorzysanie z dostępnych w Internecie baz deskryptorów, np. [<https://www.nomoreransom.org/pl/index.html>].

Nie wdając się w ocenę prawną i moralną takiej decyzji, możliwe jest także zapłacenie okupu przestępcom czy to bezpośrednio, czy za pośrednictwem licznych firm oferujących odszyfrowanie zainfekowanych plików. Abstrahując już od tego, że nie mamy dostatecznej liczby odpowiednio wykwalifikowanych kryptoanalityków, by zapewnić możliwość istnienia tak dużej liczby firm oferujących tego typu usługi, to jeszcze rezultaty takich usług pojawiają się zdecydowanie zbyt szybko w stosunku do czasu, jaki byłby niezbędny dla ich osiągnięcia metodami kryptoanalitycznymi bez współpracy z przestępcami. Ponadto firmy te, poza iluzją niezapłacenia okupu, wystawiają normalną fakturę na usługę, co dla wielu ofiar jest atrakcyjnym rozwiązaniem problemu zaksięgowania bitcoina posłanego в тридевятый паханат*, a także obniżają ryzyko nieodszyfrowania danych pomimo zapłacenia okupu.

W plikach mogą też być ukrywane inne dane, niezgodne z typem danego pliku. Szczególnie często do przenoszenia ukrytych danych, np. złośliwego kodu wykonywalnego, ale też i ukrytej informacji wykorzystywane są pliki graficzne. Cechują się one dużą odpornością na dołączanie do nich obcej zawartości i ta zawartość może łatwo pozostać niezauważona, o ile nie spowoduje zwiększenia objętości tego pliku do rozmiarów zwracających uwagę. W podobny sposób można ukrywać dane też w plikach audio lub video. Zwłaszcza, że w przypadku tych ostatnich nie trzeba się zanadto przejmować dużym rozmiarem pliku.

Innym sposobem ukrywania informacji mogą być alternatywne strumienie danych systemu NTFS (*New Technology File System*). Zwykle są one wykorzystywane dla przechowywania krótkich informacji o pliku, np. o jego pochodzeniu i są przechowywane rezydentnie w pliku \$MFT (*Master File Table*), ale też mogą opisywać zupełnie inny plik umieszczony w określonych klastrach partycji. Z praktycznego punktu widzenia, alternatywne strumienie danych NTFS są dodatkowymi, nazwanymi atrybutami danych (0x80) i ich obecność łatwo zauważyć weryfikując rekord \$MFT opisujący dany plik.

* Тридевятое (lub тридесятое) государство (царство/королевство) – odległa, bajkowa kraina leżąca „za górami, za lasami”. Паханат (od пахан — przywódca grupy przestępczej) – kraina rządzona przez przestępcę.

Kolejnym aspektem, na który warto zwrócić uwagę, są techniki steganograficzne zmierzające do ukrycia nie tylko treści, ale i samego faktu istnienia pewnej informacji. Najpopularniejszą z technik steganograficznych jest technika najmniej znaczących bitów (LSB – *Least Significant Bit*) [Fetah, Rezvani, Irani 2021]. Wykorzystuje ona pliki graficzne, audio lub video i polega na takiej modyfikacji najmniej znaczących bitów kodujących obraz lub dźwięk, żeby ukryć w nich tajną informację. Wykrycie tej techniki jest trudne, gdyż tak zmodyfikowany plik otwiera się poprawnie, a modyfikacje w tak nieznaczny sposób zniekształcają obraz lub dźwięk, że jest to praktycznie niemożliwe do wykrycia przez nieświadomego odbiorcę.

Jeszcze jedną techniką kontrwykrywczą są zmiany sygnatur i rozszerzeń plików oraz umieszczanie ich w lokalizacjach, gdzie ich obecność może pozostać niezauważona. Zmiana sygnatury na inną, niż właściwa dla danego typu pliku, zwłaszcza na nic nieznaczący ciąg znaków, chroni go przed znalezieniem przez automaty programów do odzyskiwania danych. Natomiast nadanie nierzucającej się w oczy nazwy, zmiana rozszerzenia np. na *.dll i umieszczenie pliku w którymś z katalogów systemu operacyjnego minimalizuje ryzyko, że analityk zainteresuje się nim podczas analizy manualnej, np. przy okazji zakończonej niepowodzeniem próby otwarcia zamaskowanego w ten sposób pliku.

5. Podsumowanie

Fizyczne możliwości odzyskiwania danych wykraczają daleko poza rezultaty uzyskiwane z wykorzystaniem dostępnych narzędzi i powszechnie znanych metod postępowania. Jednak wykorzystanie tego potencjału wymagałoby prowadzenia systematycznych badań w wybranych kierunkach, co wymagałoby spojrzenia na zagadnienie odzyskiwania danych z długofalowej perspektywy, kompleksowego podejścia oraz konsekwentnego zabezpieczania finansowania realizacji kolejnych projektów. I trudno się spodziewać, by w przewidywalnej przyszłości takie badania zostały podjęte.

Realnie przesuwanie granic tego, co praktycznie wykonalne w kierunku tego, co fizycznie możliwe musi się odbywać małymi krokami. Takim krokiem może być każde wyjście poza utarte ścieżki, poszukiwanie rozwiązania problemu tam, gdzie przeklikiwanie zautomatyzowanych procedur nie przynosi rezultatu, prowadzenie manualnych analiz i weryfikacja wyników zwracanych przez dostępne narzędzia. Warto takie działania podejmować, bo często włożenie nawet niewielkiego dodatkowego wysiłku pozwala uzyskać znacznie lepsze rezultaty, a w pewnych sytuacjach wyłącznie od staranności i umiejętności operatora zależy, czy jakieś rezultaty w ogóle się pojawią.

Dla podnoszenia skuteczności odzyskiwania danych kluczowe znaczenie ma zrozumienie zasad działania nośników danych oraz ich struktury logicznej. To one są fundamentem dla skutecznej diagnostyki, która z kolei w istotny sposób wpływa na dobór właściwych metod rozwiązania problemu, zwiększa szanse powodzenia procesu oraz minimalizuje ryzyko błędów i zbędnych ingerencji. Zrozumienie pozwala też na odróżnienie tego, co naprawdę niemożliwe od tego, co tylko trudne.

Niestety odzyskiwanie danych jest mocno zaniedbywaną i lekceważoną dziedziną, a przez to wymagającą znacznego wkładu własnej nauki i pracy. Konieczne przy tym są umiejętności analityczne oraz odpowiednia weryfikacja i selekcja materiałów do nauki. Tym bardziej, że

nieprawdziwe, niekiedy wręcz szkodliwe informacje można znaleźć nie tylko na niskiej wartości merytorycznej internetowych forach, ale i w szkolnych podręcznikach [Kaczmarzyk 2024a].

Kwestia zrozumienia, zdobywania doświadczenia i podnoszenia kompetencji jest tym bardziej istotna, że błędy w odzyskiwaniu danych często są nieodwracalne. Dlatego też do nauki i eksperymentów należy wykorzystywać dyski, na których nie ma niczego istotnego, unikając ryzykownych działań na dyskach zawierających ważne dane, w szczególności – materiał dowodowy. Wobec różnorodności modeli nośników danych, rozwiązań konstrukcyjnych i oprogramowania układowego oraz występujących w nich usterek nie można spodziewać się, że ktokolwiek będzie w stanie zawsze uniknąć błędów, jednak należy wykorzystać wszystkie dostępne możliwości, by minimalizować ryzyko pomyłek.

Rozwijanie zrozumienia, doświadczenia i samodzielności w odzyskiwaniu danych ma też istotne znaczenie w kontekście powszechnie wykorzystywanych wysoko zaawansowanych narzędzi, a zwłaszcza ich pochodzenia. Trzeba mieć świadomość tego, że tak zaawansowane narzędzia są opracowywane i rozwijane w znacznym stopniu na zlecenie, przy współpracy i pod kontrolą służb specjalnych niekoniecznie sojusznicy, a w pewnych przypadkach wręcz otwarcie wrogich państw. Niektóre z tych firm zostały założone i są prowadzone przez funkcjonariuszy (choćby i formalnie byłych) służb oraz zatrudniają funkcjonariuszy jako kluczowy personel. Jest to istotne zwłaszcza w sytuacjach korzystania ze wsparcia technicznego producentów, kiedy oddanie zdalnego dostępu technikowi może być równoznaczne z zaproszeniem do wycieku danych.

Zdobywanie rzetelnej wiedzy technicznej o nośnikach danych ma krytyczne znaczenie dla specjalistów bezpośrednio zajmujących się odzyskiwaniem danych, ale podstawowa znajomość tych zagadnień jest ważna także dla funkcjonariuszy zabezpieczających urządzenia w celu przekazania ich do laboratorium. Ogólna orientacja w tej tematyce przyda się też przełożonym oraz nadzorującym postępowania prokuratorom, gdyż fantastyczne oczekiwania oparte o różne baśnie i legendy nie pomagają w pracy i często bywają przyczyną rozczarowań.

Literatura

1. Amer, A., Holliday, J., Long, D. D. E., Miller E. L., Paris, J-F., Schwartz, T. S. J.: *Data Management and Layout for Shingled Magnetic Recording*, „IEEE Transactions on Magnetics”, 47(10), (2011).
2. Baraniecki, P.: *Czas (nie) jest najprostszą rzeczą*, Zwalczenie Przystępczości Internetowej, Sanok (2025a).
3. Baraniecki, P.: *Smartfon i „biling” nie są jedynymi źródłami informacji* [w] Matyniak, G. [red.] *Zwalczenie przystępczości internetowej*, Uczelnia Państwowa im. Jana Grodka, Sanok (2025b).
4. Bertram, H. N.: *Theory of Magnetic Recording*, Cambridge University Press, London (1994).
5. Bitter, F.: *Experiments on the Nature of Ferromagnetism*, “Physical Review” 41(507), (1932).
6. Chan, K. S., Radhakrishnan, R., Eason, K., Elidrissi, M. R., Miles, J. J., Vasic, B., Krishnan, A. R.: *Channel models and detectors for two-dimensional magnetic recording*. “IEEE Transactions on Magnetics”, 46(3), (2010).

7. Chen, B. M., Lee, T. H., Peng, K., Venkataramanan, V.: *Hard Disk Drive Servo Systems*, Springer-Verlag, London, (2006).
8. Chiang M.-L., Lee, P. C. H., Chang, R.-Ch.: *Using data clustering to improve cleaning performance for flash memory*, „Software: Practice and Experience” 29(3), (1999).
9. Davies, G.: *Vehicle forensics best practice and future direction*, Flash Data Recovery and Digital Forensic Summit, Warszawa (2024).
10. De Nardi, C., Desplats, R., Perdu, P., Beaudoin, F., Gauffier, J-L.: *Oxide charge measurements in EEPROM devices*, „Microelectronics Reliability” 45 (2005).
11. Dieny, B., Goldfarb, R. B., Lee, K.-J.: *Introduction to Magnetic Random Access Memory*, IEEE Press, Piscataway, (2017).
12. Du, C., Pang, C. K., *Multi-Stage Actuation Systems and Control*, CRC Press, Boca Raton, (2019).
13. Fetah, M., Rezvani, M., Irani, Y.: *A New Method of Coding for Steganography Based on LSB Matching Revisited*, „Security and Communications Network” 5 (2021).
14. Fukami, A.: *Exploiting the eMMC security features using the VNR*, Flash Data Recovery & Digital Forensic Summit Warszawa (2024).
15. Gomez, R., Adly, A., Mayergoyz, I., Burke, E.: *Magnetic Force Scanning Tunnelling Microscope Imaging of Overwritten Data*, “IEEE Transactions on Magnetics” 28(5), (1992).
16. Gomez, R., Burke, E., Adly, A., Mayergoyz, I., Gorczyca, J.: *Microscopic Investigations of Overwritten Data*, “Journal of Applied Physics” 73(10), 6001 (1993).
17. Gupta, M. R., Hoeschele, M. D., Rogers, M. K: *Hidden Disk Areas: HPA and DCO*. “International Journal of Digital Evidence” 5(1), (2006).
18. Hanzii, D., Kelm, E., Luapunov, N., Milovanov, R., Molodcova, G., Yanul, M., Zubov, D., *Determining the state of non-volatile memory cell of floating gate using scanning probe microscopy*, „Proceedings of the SPIE”, Volume 8700 (2013).
19. <https://flashboot.ru/> [dostęp 24 lutego 2026 r.].
20. <https://kaleron.edu.pl/vykorystannia-poszkodzenych-blokiv-mahnitnykh-holovok-u-vidnovlenni-danykh.php> [dostęp 24 lutego 2026 r.].
21. <https://kaleron.pl/awarie-SSD.php> [dostęp 24 lutego 2026 r.].
22. <https://t13.org/index.php/standards-published> [dostęp 24 lutego 2026 r.].
23. <https://www.nomoreransom.org/pl/index.html> [dostęp 24 lutego 2026 r.].
24. <https://www.t10.org/scsi-3.htm> [dostęp 24 lutego 2026 r.].
25. <https://www.usbdev.ru/> [dostęp 24 lutego 2026 r.].
26. Hughes, G. F., Commins, D. M., Coughlin, T.: *Disposal of disk and tape data by secure sanitization*, “IEEE Security and Privacy”, 7(4), (2009).
27. Hwang, E., Oenning, T., Mathew, G., Rahgozar, P., Tedja, S., Fang, H., Garfunkel, G., Wu, Y., Hu, D., Duquette, P., Fitch, K., Rabbitt, C., Petrizzi, J., Wilson, B., Rauschmayer, R.: *Skew-Dependent Performance Evaluation of Array-Reader-Based Magnetic Recording With Dual-Reader*, “IEEE Transactions on Magnetics” 51(4), (2015).

28. Jiang, B.-Y., Zhang, K., Machita, T., Chen, W., Dovek, M.: *Tunneling magnetoresistive device as read heads in hard disk drives*, „Journal of Magnetism and Magnetic Materials” 571 (2023).
29. Kaczmarzyk, P.: *Jak błędy w podręcznikach informatyki wpływają na wiedzę uczniów?* „Security Magazine” 9(30), (2024a).
30. Kaczmarzyk, P.: *Jak przewidzieć awarię SSD*, „Security Magazine” 2(23), (2024b).
31. Kaczmarzyk, P.: *Możliwości odzyskiwania filmów z kamer i aparatów*, The Hack Summit, Warszawa (2025a).
32. Kaczmarzyk, P.: *Niszczenie danych – regulacje, a rzeczywista skuteczność*, Security Management Audit Forum „Semafor”, Warszawa (2024c).
33. Kaczmarzyk, P.: *Podstawy diagnostyki dysków twardych*, „Security Magazine” 2(11), (2023a).
34. Kaczmarzyk, P.: *Przyznajemy Nagrodę Gutmanna*, Advanced Threat Summit, Warszawa (2025b).
35. Kaczmarzyk, P.: *Rodzaje uszkodzonych sektorów*, „Security Magazine” 7(28), (2024d).
36. Kaczmarzyk, P.: *Rola metadanych w przechowywaniu plików*, „Security Magazine” 5(14), (2023b).
37. Kaczmarzyk, P.: *SMART w diagnostyce i monitoringu dysków*, „Security Magazine” 8(29), (2024e).
38. Kaczmarzyk, P.: *TRIM w dyskach SMR i SSD*, The Hack Summit, Warszawa (2024f).
39. Kaczmarzyk, P.: *Wyrzucamy algorytm Gutmanna do kosza*, The Hack Summit, Warszawa (2023c).
40. Kaczorowski, A., Budaszewski, R., Kalisiak, S., Krać-Batyra, A., Sidor, T.: *Podejrzenie seksualnego wykorzystania dziecka*, „Gazeta Policyjna” 1(61), (2026).
41. Kanai, Y., Jinbo, Y., Tsukamoto, T., Greaves, S. J., Yoshida, K., Muraoka, H.: *Finite-Element and Micromagnetic Modeling of Write Heads for Shingled Recording*, “IEEE Transactions on Magnetics”, 46(3), (2010).
42. Khatami, S. M., Vasić, B.: *Generalized Belief Propagation Detector for TDMR Microcell Model*, “IEEE Transactions on Magnetics” 49(7), (2013).
43. Khizroev, S., Litvinov, D.: *Perpendicular magnetic recording*, Kluwer Academic Publishers, Dordrecht (2004).
44. Li, H., Liu, B., Hua, W., Chong, T-C.: *Intermolecular force, surface roughness, and stability of head-disk interface*, “Journal of Applied Physics” 97 (2005).
45. Lin, S., Costello, D. J.: *Error control coding*, Pearson Education Inc., Upper Saddle River (1983).
46. Mallinson, J. C.: *Magneto-Resistive and Spin Valve Heads*, Academic Press, San Diego, (2002).
47. Mamun, al, A., Guo, G. X., Bi, Ch.: *Hard Disk Drive Mechatronics and Control*, CRC Press, Boca Raton, (2006).
48. Mansuripur, M., Sincero, G.: *Principles and Techniques of Optical Data Storage*, „Proceedings of the IEEE” 85(11), (1997).
49. Mayergoyz, I. D., Tse, C.: *Spin-stand Microscopy of Hard Disk Data*. Elsevier Science Ltd., Amsterdam (2007).

50. Micheloni, R., Crippa, L., Marelli, A.: *Inside NAND Flash Memories*, Springer, Dordrecht (2010).
51. Miura, K., Yamamoto, E., Aoi, H., Muraoka, H.: *Skew angle effect in shingled writing magnetic recording*, „Physics Procedia” 16, (2011).
52. Moreira, J. C., Farrell, P. G., *Essentials of Error Control Coding*, John Wiley & Sons, Ltd., Chichester (2006).
53. Nikkel, B., *Metody zabezpieczenia cyfrowego*, tłum. K. Kulczycki, Wydawnictwo Naukowe PWN S. A., Warszawa (2021).
54. Ning, S., Luo, J.: *Demonstration and Understanding of Nano-RAM Novel One-Time Programmable Memory Application*, “IEEE Transactions on Electron Devices” 66(5), (2019).
55. Nishi, Y.: *Advances in Non-volatile Memory and Storage Technology*, Elsevier, Cambridge, (2014).
56. Patterson, D. A., Gibson, G., Katz, R. H.: *A Case for Redundant Arrays of Inexpensive Disks (RAID)*, „ACM SIGMOD Record” 17(3), (1988).
57. Pawlikowski, M.: *Flash – how to make life easier. Tips and tricks, Flash Data Recovery & Digital Forensic Summit*, Warszawa (2024).
58. Pawlikowski, M.: *Where is the limit? Analysis of devices from maritime disasters. Flash Data Recovery & Digital Forensic Summit* Warszawa (2023).
59. Redaelli, A.: *Phase Change Memory Device Physics, Reliability and Applications*, Springer, Cham, (2018).
60. Riggall, C. M., McCarthy, S. G.: *Design of Error Correction Systems for Disk Drives*, “IEEE Transactions on Magnetics” 34(4), (1998).
61. Ruemmler, Ch., Wilkes, J.: *An introduction to disk drive modeling*, „IEEE Computer 27(3)”, (1994).
62. Schouhamer Immink, K. A.: *Codes for Mass Data Storage Systems*, Shannon Foundation Publishers, Eindhoven (2004).
63. Sheremetov, S.: *Vehicle forensic, IoT and embedded file systems*, Flash Data Recovery and Digital Forensic Summit, Warszawa (2023).
64. Sobey, Ch. H.: *Drive-Independent Data Recovery: The Current State-of-the-Art*, “IEEE Transactions on Magnetics” 42(2), (2006).
65. Sołodow, I. A.: *Mechanizm działania dysku twardego typu HDD i możliwości odzyskiwania danych po jego uszkodzeniu*, „Prokuratura i Prawo” 3. (2018)
66. Sweeney, P.: *Error control coding. From theory to practice*, John Wiley & Sons, Ltd., Chichester (2002).
67. Šestanji I.: *NAND Flash Data Recovery Cookbook*, Igor Šestanji, Belgrade (2016).
68. Thirumalai, G. K., *A Beginner’s Guide to SSD Firmware: Designing, Optimizing, and Maintaining SSD Firmware*, Apress, San Jose (2023).
69. Uematsu, Y., Fukushi, M.: *Servo track writing technology*, “Fujitsu Scientific & Technical Journal”, 37(2), (2001).
70. Vasić, B., Kurtas, E. M.: *Coding and signal processing for magnetic recording systems*, CRC Press LLC, Boca Raton (2005).

71. Wright, C., Kleiman, D., Shyaam Sundhar, R. S.: *Overwriting Hard Drive Data: The Great Wiping Controversy*. R. Sekar and A.K. Pujari (Eds.): ICISS 2008, LNCS 5352, Springer-Verlag Berlin Heidelberg (2008).
72. Wu, Z.: *Coding and Iterative Detection for Magnetic Recording Channels*, Springer Science + Business Media LLC, New York (2000).
73. Yamada, T., Fukushi, M., Suzuki, H., Takaishi, K.: *Servo track writing technology*, "Fujitsu Scientific & Technical Journal", 42(1), (2006).
74. Агалиди, Ю. С., Кожухарь, П. В., Левый, С. В., Мачнев, А. М., Пономарёв, С. Л.: *Исследование индуцированных магнитных полей рассеяния тонкоплёночных дисперсных ферромагнетиков*, „Известия высших учебных заведений. Радиоэлектроника” т. 55 № 5(559) (2012).
75. Кожневский, С. Р.: *Аппаратные методы восстановления информации, хранимой на жёстких дисках*, “Реєстрація, зберігання та обробка даних”. Том 4, № 2, (2002).
76. Кожневский, С. Р.: *Взгляд на жёсткий диск "изнутри". Визуальный анализ*. ООО "ЕПОС", Київ, (2004).
77. Кожневский, С. Р.: *Взгляд на жёсткий диск "изнутри". Магнитные головки*, ООО "ЕПОС", Київ (2009).
78. Кожневский, С. Р.: *Взгляд на жёсткий диск "изнутри". Механика и сервосистема*, ООО "ЕПОС", Київ (2007).
79. Кожневский, С. Р.: *Взгляд на жёсткий диск "изнутри". Основы хранения информации*, ООО "ЕПОС", Київ (2005).
80. Кожневский, С. Р., Левый, С. В., Вишневский, В. С., Прокопенко, С. Д.: *Методы визуализации магнитных полей носителей информации. Информационная безопасность офиса. Научно — практический сборник. Выпуск первый. «Технические средства защиты информации»*, К.:ООО «ТИД ДС» (2003).
81. Кожневский, С., Прокопенко, С., Гайшинец, В.: *Восстановление информации на жёстких дисках с заклинившим шпиндельным двигателем*, “Реєстрація, зберігання та обробка даних”, том 10, №4, (2008).
82. Сенкевич, Г. Е.: *Искусство восстановления данных*, БХВ-Петербург, Санкт Петербург, (2011).
83. Ташков П. А.: *Восстанавливаем данные на 100%*, Питер, Санкт Петербург (2010).

Marlena Kruczek¹

Wyzwania etyczne w pracy biegłego sądowego – bezstronność czy presja instytucjonalna?

Abstrakt/Streszczenie

Praca poświęcona jest analizie wyzwań etycznych występujących w pracy biegłego sądowego, ze szczególnym uwzględnieniem konfliktu pomiędzy obowiązkiem zachowania bezstronności, a presją instytucjonalną. Omówiono rolę biegłego w postępowaniu sądowym oraz znaczenie zasad etycznych, takich jak obiektywizm, niezależność, rzetelność i odpowiedzialność zawodowa. Przedstawiono również zagrożenia mogące wpływać na jakość i wiarygodność opinii, w tym naciski ze strony uczestników postępowania, ograniczenia organizacyjne oraz konflikty interesów.

W pracy zwracam szczególną uwagę na brak jednolitego kodeksu etyki biegłych sądowych w Polsce oraz wynikające z tego trudności w interpretacji i stosowaniu standardów etycznych. Uzupełnieniem rozważań teoretycznych jest analiza wyników anonimowej ankiety przeprowadzonej wśród biegłych sądowych.

Przeprowadzona analiza pozwala stwierdzić, że etyczna postawa biegłego sądowego ma kluczowe znaczenie dla wiarygodności opinii oraz prawidłowego funkcjonowania wymiaru sprawiedliwości.

Słowa kluczowe: biegły sądowy, etyka zawodowa, bezstronność, presja instytucjonalna, opinia biegłego, wymiar sprawiedliwości.

Wstęp – Praca biegłego sądowego – analiza problemów etycznych

Praca biegłego sądowego odgrywa niezwykle istotną rolę w funkcjonowaniu wymiaru sprawiedliwości. To właśnie opinie specjalistów z różnych dziedzin często stanowią jeden z kluczowych elementów wpływających na decyzje podejmowane przez Sąd. Od biegłego wymaga się nie tylko wysokich kwalifikacji zawodowych i specjalistycznej wiedzy, ale też przestrzegania zasad etycznych, takich jak bezstronność, rzetelność oraz niezależność. Jak wskazuje M. Skorecki, działalność biegłego sądowego wymaga nie tylko kompetencji zawodowych, ale również przestrzegania podstawowych norm etycznych i odpowiedzialności za wydawaną opinię². W praktyce jednak wykonywanie tej funkcji wiąże się z wieloma trudnościami oraz dylematami moralnymi.

Biegły funkcjonuje w środowisku, w którym może doświadczać różnego rodzaju presji – zarówno ze strony instytucji, uczestników postępowania, jak i ograniczeń organizacyjnych czy czasowych. W takich warunkach zachowanie pełnego obiektywizmu staje się nie tylko obowiązkiem zawodowym, ale także wyzwaniem etycznym. Szczególne znaczenie ma odpowiedzialność biegłego za wydawaną opinię, ponieważ jej treść może wpływać na sytuację życiową i majątkową, a nawet wolność innych osób.

¹ Marlena Kruczek – Biegły Sądu Okręgowego w Krakowie z zakresu informatyki śledczej i analizy kryminalnej. Od blisko dwudziestu lat związana z e-Detektywi sp. z o.o.

² Skorecki, M. *Etyczne podstawy działania biegłych sądowych*. „Bezpieczeństwo. Teoria i Praktyka”, numer specjalny, 2008, s. 41–50.

Celem niniejszej pracy jest analiza najważniejszych problemów etycznych występujących w pracy biegłego sądowego, ze szczególnym uwzględnieniem konfliktu pomiędzy koniecznością zachowania bezstronności, a presją instytucjonalną. W pracy omówione zostaną podstawowe zasady etyki zawodowej biegłych, najczęściej pojawiające się dylematy moralne oraz konsekwencje naruszenia norm etycznych. Uzupełnieniem części teoretycznej będzie analiza wyników ankiety przeprowadzonej wśród biegłych sądowych, której celem jest poznanie ich doświadczeń i opinii dotyczących etycznych aspektów wykonywanego zawodu.

Bezstronność jako podstawa etyki

Bezstronność stanowi jedną z najważniejszych zasad etycznych w pracy biegłego sądowego. Od osoby pełniącej tę funkcję oczekuje się obiektywizmu, niezależności oraz rzetelności. Osoba pełniąca tą funkcję powinna kierować się wyłącznie wiedzą specjalistyczną oraz wynikami przeprowadzonych badań, a nie własnymi przekonaniem, emocjami czy oczekiwaniami stron postępowania. Szczególne znaczenie ma unikanie wszelkich uprzedzeń dotyczących cech osoby badanej, takich jak płeć, wiek, narodowość, wyznanie czy poglądy polityczne. Zachowanie bezstronności wymaga również świadomości własnych ograniczeń i potencjalnych konfliktów interesów. W sytuacji, gdy istnieje ryzyko utraty obiektywizmu – na przykład z powodu relacji osobistych, zależności zawodowych lub wcześniejszych kontaktów z uczestnikami postępowania – biegły powinien odmówić sporządzenia opinii³. Takie postępowanie świadczy o odpowiedzialności zawodowej oraz poszanowaniu zasad etyki.

Kodeksy etyczne oraz regulacje dotyczące pracy biegłych podkreślają, że nadrzędnym celem działalności eksperta powinno być dobro wymiaru sprawiedliwości oraz dążenie do ustalenia prawdy. Oznacza to, że biegły nie może kierować się presją ze strony zleceniodawcy, oczekiwaniami Sądu ani własnymi korzyściami. Każda wydana opinia powinna być oparta na rzetelnej analizie materiału dowodowego i zgodna z aktualną wiedzą specjalistyczną. W tym miejscu należy podkreślić, iż wskazane kodeksy i regulacje zazwyczaj tworzone są przez prywatne instytucje lub związki czy towarzystwa zawodowe, dla przykładu Polskie Towarzystwo Psychologiczne⁴.

Brak bezstronności może prowadzić do poważnych konsekwencji zarówno dla uczestników postępowania, jak i dla samego wymiaru sprawiedliwości. Nierzetelna lub stronnicza opinia może wpłynąć na treść wyroku, a tym samym naruszyć prawa osób uczestniczących w postępowaniu. Z tego względu etyczna postawa biegłego sądowego ma kluczowe znaczenie dla zachowania zaufania społecznego do instytucji sądowych.

Presja instytucjonalna

Mimo założonej niezależności i autonomii, zdarzyć się może, że praca biegłego odbywa się pod wpływem różnorodnych form presji instytucjonalnej. Może to wynikać zarówno z oczekiwań organów ścigania czy stron postępowania, jak i z warunków organizacyjnych związanych z przebiegiem procesu. W praktyce biegły niejednokrotnie znajduje się w sytuacji konfliktu pomiędzy obowiązkiem zachowania pełnej bezstronności, a oczekiwaniami dotyczącymi treści lub kierunku wydawanej opinii.

³ Studzińska, J., & Dzierżanowska, J. *Biegli w postępowaniu sądowym cywilnym i karnym*. Warszawa: Wolters Kluwer, 2019.

⁴ <https://psych.org.pl/certyfikaty-i-rekomendacje/rekomendacje-bieglych-sadowych> [ostatni dostęp: 12.06.2026].

Presja instytucji, dla której wykonywana jest ekspertyza, może przyjmować różne formy. Często dotyczy konieczności sporządzenia opinii w bardzo krótkim czasie, z ograniczonym dostępem do materiału dowodowego lub sugestii dotyczących oczekiwanych wniosków ekspertyzy⁵. Zdarza się również, że strony postępowania próbują wpływać na sposób interpretacji wyników ekspertyzy lub przedstawiania osoby badanej, czy też podważyć wiarygodność danych uzyskanych w trakcie przygotowywania ekspertyzy np. urządzeń mobilnych, dysków twardych czy innych dowodów elektronicznych. W takich sytuacjach istnieje ryzyko uproszczenia obrazu badanego, pomijania istotnych informacji zawartych w aktach sprawy czy formułowania wniosków zgodnych z oczekiwaniami zlecniodawcy. Szczególnie niebezpieczne mogą być sytuacje, w których presja ekonomiczna lub zawodowa prowadzi do naruszenia zasad etyki. Problem ten może nasilać się w przypadku prywatnych ekspertyz, gdzie pojawia się ryzyko zależności finansowej od zlecającego opinię. W skrajnych przypadkach może to prowadzić do zjawisk takich jak korupcja, płatna protekcja czy świadome wydawanie nierzetelnych opinii.

Presja instytucjonalna stanowi poważne zagrożenie dla wiarygodności pracy biegłego sądowego oraz dla prawidłowego funkcjonowania wymiaru sprawiedliwości. Dlatego tak istotne jest wzmacnianie standardów etycznych, zwiększanie kontroli jakości opinii oraz zapewnienie biegłym odpowiednich warunków do niezależnego wykonywania swoich obowiązków.

Analiza wyników ankiety

W celu poznania opinii dotyczących etycznych aspektów pracy biegłego sądowego przeprowadzono anonimową ankietę wśród osób pełniących tę funkcję czynnie, jak i w przeszłości⁶. W badaniu udział wzięło 20 respondentów reprezentujących głównie zakres informatyki śledczej i analizy kryminalnej. Większość badanych posiadała wieloletnie doświadczenie zawodowe – przeważały osoby pełniące funkcję biegłego ponad 10 lat.

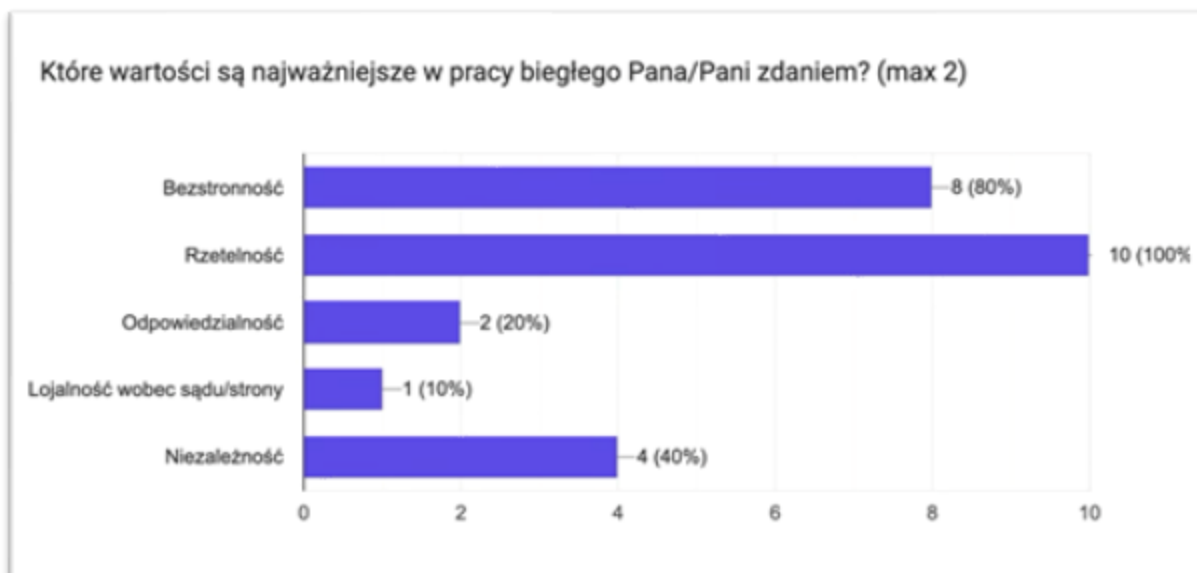
Uzyskane odpowiedzi wskazują, że problematyka etyczna jest istotnym elementem pracy biegłego sądowego. Większość respondentów zadeklarowała, że spotkała się w swojej pracy z dylematami etycznymi, przy czym część osób wskazała, że sytuacje takie występują wielokrotnie. Pokazuje to, że wykonywanie funkcji biegłego wiąże się nie tylko z odpowiedzialnością merytoryczną, ale również z koniecznością podejmowania trudnych decyzji moralnych.

Respondenci, jako najważniejsze wartości w pracy biegłego, najczęściej wskazywali bezstronność, rzetelność oraz niezależność. Wyniki te potwierdzają, że podstawą pracy eksperta pozostaje bezstronność i rzetelność wydawanej opinii. Jednocześnie część ankietowanych przyznała, że odczuwa presję ze strony uczestników postępowania, co może utrudniać zachowanie pełnej niezależności, a co za tym idzie stosowanie się do norm etycznych.

Istotnym zagadnieniem okazał się wpływ systemu wynagradzania na niezależność biegłych. Znaczna część respondentów uważa, że sposób wynagradzania może oddziaływać na obiektywizm opinii lub stwarzać ryzyko zależności od zlecniodawcy. Ankietowani wskazywali także na występowanie konfliktów interesów oraz brak jednoznacznych wytycznych etycznych w niektórych dziedzinach specjalistycznych.

⁵ Powirska-Bała, M. *Dowód z opinii biegłego – współczesne trudności i wyzwania na gruncie polskiego procesu karnego*. „Studia Prawnoustrojowe”, nr 62, 2023.

⁶ *Badanie własne przeprowadzone wśród biegłych sądowych w maju 2026 roku.*

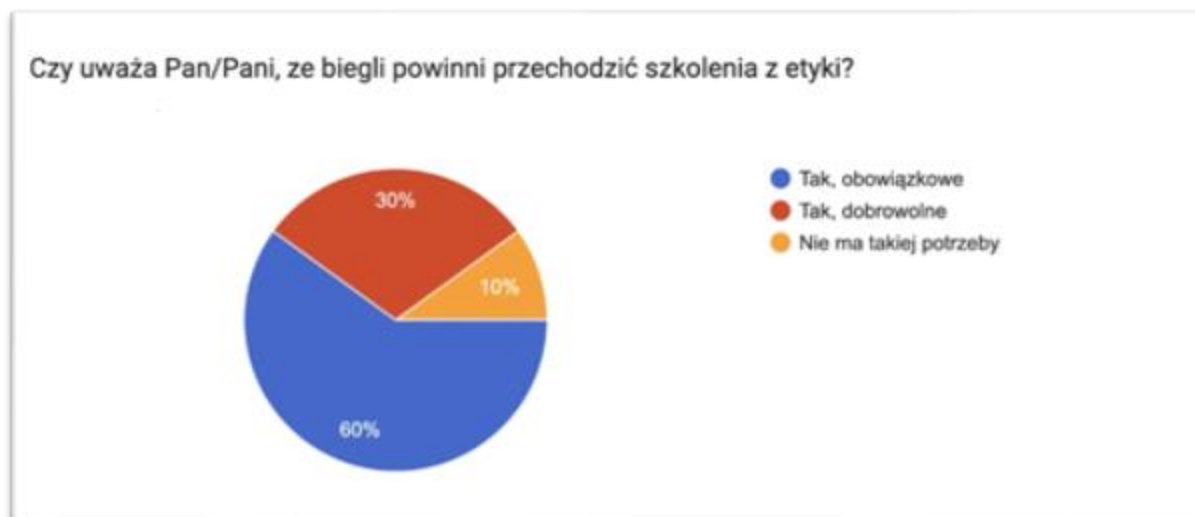


Rys. 1. Struktura odpowiedzi badanych w zakresie wartości w pracy biegłego sądowego

Źródło: Badanie własne, 2026

W sytuacjach budzących wątpliwości etyczne respondenci najczęściej deklarowali kierowanie się własnym doświadczeniem, analizą przepisów oraz konsultacjami z innymi specjalistami. Większość badanych uznała również, że biegli sądowi powinni uczestniczyć w szkoleniach z zakresu etyki zawodowej, w formie obowiązkowej lub dobrowolnej.

Za największe zagrożenia dla etyki w pracy biegłego respondenci uznali presję czasu, naciski ze strony uczestników postępowania, niskie wynagrodzenia oraz brak skutecznej kontroli jakości opinii. Odpowiedzi te pokazują, że problemy etyczne wynikają nie tylko z indywidualnych postaw biegłych, ale również z warunków organizacyjnych funkcjonowania wymiaru sprawiedliwości.



Rys. 2. Struktura odpowiedzi badanych w zakresie szkoleń z etyki dla biegłych sądowych

Źródło: Badanie własne, 2026

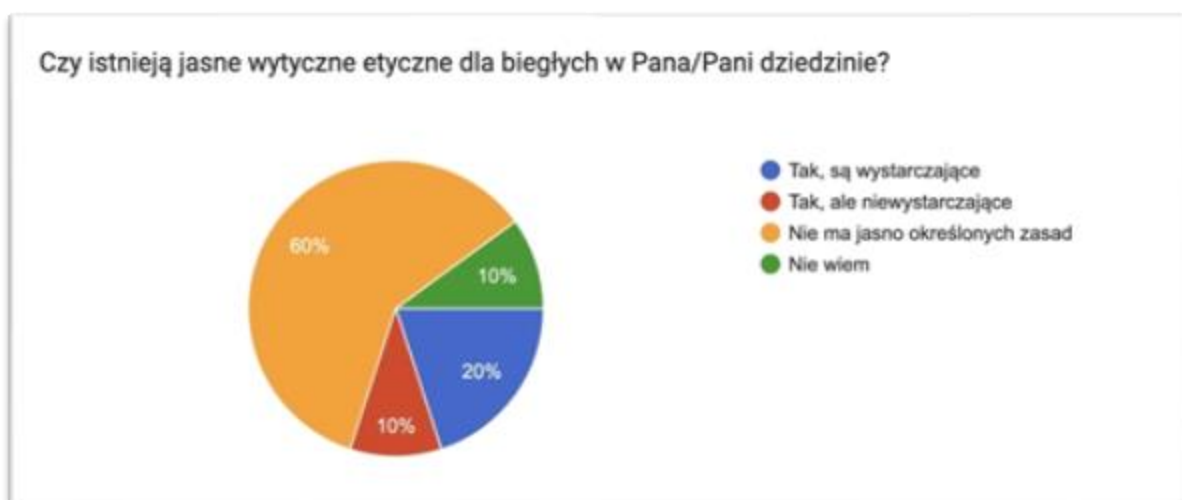
Przeprowadzona ankieta potwierdza, że etyka zawodowa odgrywa kluczową rolę w pracy biegłego sądowego. Zachowanie bezstronności i niezależności wymaga nie tylko odpowiednich kompetencji zawodowych, ale także odporności na presję instytucjonalną oraz wysokiego poziomu odpowiedzialności moralnej.

Rozwiązania etyczne i sposoby wzmacniania niezależności biegłych sądowych

W obliczu licznych wyzwań etycznych związanych z wykonywaniem powyższej funkcji szczególnego znaczenia nabiera potrzeba stosowania zasad, które pozwalają zachować niezależność, rzetelność oraz obiektywizm wydawanych opinii. Podstawowym obowiązkiem biegłego powinno być ograniczanie treści opinii wyłącznie do faktów wynikających z materiału dowodowego oraz posiadanej wiedzy specjalistycznej. Ekspert nie powinien przejmować roli sędziego, prokuratora czy obrońcy, ponieważ jego zadaniem jest dostarczenie fachowej analizy, a nie rozstrzygnięcie o winie lub odpowiedzialności stron postępowania.

Istotnym elementem etycznego wykonywania zawodu jest także świadomość własnych kompetencji i ograniczeń. Biegły powinien podejmować się sporządzania opinii wyłącznie w zakresie posiadanej specjalizacji i doświadczenia zawodowego. W sytuacji braku wystarczającej wiedzy lub możliwości zachowania pełnej bezstronności powinien on odmówić przyjęcia zlecenia. Powyższe działanie świadczy nie o braku kompetencji, lecz o odpowiedzialności zawodowej i poszanowaniu zasad etycznych.

Ważną rolę w ograniczaniu problemów etycznych odgrywa też korelacja pomiędzy normami prawnymi, a zasadami etyki zawodowej. Przepisy prawa określają podstawowe obowiązki i odpowiedzialność biegłego, jednak nie są w stanie przewidzieć wszystkich sytuacji niejasnych pojawiających się w praktyce. Dlatego znaczenie mają nieformalne standardy środowiskowe, doświadczenie zawodowe oraz indywidualne poczucie odpowiedzialności moralnej.



Rys.3. Struktura odpowiedzi badanych w zakresie wytycznych etycznych dla biegłych sądowych

Źródło: Badanie własne 2026

Jednym z problemów funkcjonujących w Polsce jest brak jednolitego kodeksu etyki biegłych sądowych, który obejmowałby wszystkie specjalizacje. Obecnie poszczególne grupy zawodowe często kierują się własnymi regulacjami lub ogólnymi zasadami etyki zawodowej, co może prowadzić do niejednorodnych standardów postępowania. Brak spójnych wytycznych utrudnia także ocenę zachowań nieetycznych oraz odpowiedzialności zawodowej biegłych.

W celu zwiększenia jakości i wiarygodności opinii coraz częściej podkreśla się potrzebę organizowania szkoleń z zakresu etyki zawodowej, komunikacji oraz odpowiedzialności prawnej dla tej grupy. Istotne znaczenie mogłoby mieć również wprowadzenie bardziej przejrzystych zasad oceny jakości opinii oraz skuteczniejszych mechanizmów kontroli pracy ekspertów.

Działania takie mogłyby przyczynić się do wzmocnienia zaufania społecznego wobec biegłych sądowych i całego wymiaru sprawiedliwości.

Zatem, rozwiązanie problemów etycznych w pracy biegłego sądowego wymaga nie tylko odpowiednich regulacji prawnych, ale również rozwijania świadomości etycznej samych ekspertów. Tylko połączenie wiedzy specjalistycznej, odpowiedzialności zawodowej oraz niezależności może zapewnić rzetelność opinii i prawidłowe funkcjonowanie procesu sądowego.

Podsumowanie

Praca biegłego sądowego stanowi niezwykle ważny element funkcjonowania wymiaru sprawiedliwości. Opinie sporządzane przez ekspertów często mają istotny wpływ na przebieg postępowania oraz treść wydawanych wyroków, dlatego od tej grupy wymaga się nie tylko wysokich kompetencji zawodowych, ale również przestrzegania zasad etycznych. Szczególne znaczenie mają takie wartości jak bezstronność, rzetelność, niezależność oraz odpowiedzialność za wydawaną opinię.

Celem niniejszej pracy była analiza wyzwań etycznych pojawiających się w pracy biegłego sądowego, ze szczególnym uwzględnieniem konfliktu pomiędzy koniecznością zachowania obiektywizmu, a presją instytucjonalną. Rozważania teoretyczne oraz wyniki przeprowadzonej ankiety pokazują, że wykonywanie powyższej funkcji wiąże się z licznymi dylematami moralnymi i wymaga dużej odporności na wpływy zewnętrzne.

Przeprowadzone badania potwierdziły, że biegli sądowi dostrzegają znaczenie etyki zawodowej oraz są świadomi odpowiedzialności wynikającej z pełnionej funkcji. Jednocześnie wielu respondentów wskazało na problemy związane z presją czasu, oczekiwaniami stron postępowania, niewystarczającymi regulacjami oraz ryzykiem konfliktu interesów. Pokazuje to, że zachowanie pełnej bezstronności w praktyce nie zawsze jest łatwe i wymaga zarówno indywidualnej uczciwości, jak i odpowiednich standardów organizacyjnych.

Współczesny wymiar sprawiedliwości powinien dążyć do wzmocnienia niezależności biegłych sądowych poprzez rozwijanie jasnych zasad etycznych, systemów kontroli jakości opinii oraz szkoleń z zakresu etyki zawodowej już na etapie procedury wpisu na listę biegłych. Tylko wówczas możliwe będzie utrzymanie wysokiego poziomu zaufania społecznego do opinii ekspertów oraz do samego wymiaru sprawiedliwości.

Bibliografia

1. Dzierżanowska J., 2019, Kompetencje biegłego sądowego – wybrane problemy, „Forum Prawnicze”, nr 1 (51), s. 66–75.
2. Fras M., 2021, Odpowiedzialność deliktowa biegłego za szkodę spowodowaną wydaniem nieprawdziwej lub nieprawidłowej opinii w postępowaniu sądowym. Rozważania na tle najnowszej judykatury, „Gdańskie Studia Prawnicze”, nr 1 (49), s. 66–84.
3. <https://psych.org.pl/certyfikaty-i-rekomendacje/rekomendacje-bieglych-sadowych> [ostatni dostęp: 12.06.2026].
4. Powirska-Bała M., 2023, Dowód z opinii biegłego – współczesne trudności i wyzwania na gruncie polskiego procesu karnego, „Studia Prawnoustrojowe”, nr 62.
5. Skorecki M., 2008, Etyczne podstawy działania biegłych sądowych, „Bezpieczeństwo. Teoria i Praktyka”, numer specjalny, s. 41–50. Studzińska J., Dzierżanowska J., 2019, *Biegli*

w postępowaniu sądowym cywilnym i karnym. Praktyczne omówienie regulacji z orzecznictwem, Warszawa, wyd. Wolters Kluwer.

6. Tomaszewski T., 1998, *Dowód z opinii biegłego w procesie karnym*, Kraków, wyd. Instytut Ekspertyz Sądowych.
7. Widła T., 2005, Odpowiedzialność biegłych – nowe problemy, „Palestra”, nr 7–8.

20 lat funkcji biegłego – historia błędów większych i mniejszych

Streszczenie

W niniejszym opracowaniu przedstawione zostały wybrane przypadki nieprawidłowości, z którymi autor zetknął podczas 20 lat opiniowania w sprawach karnych jako biegły z zakresu informatyki śledczej. Poruszone zostały problemy związane z przechowywaniem opinii i zapewnieniem dostępu do treści przekazywanych wraz z nią, jako informacje przechowywane elektronicznie. Podniesione zostały ponadto kwestie dotyczące kategoryczności wydawanych opinii oraz problemy związane z ich jakością, jak również dotyczące braku wymiany informacji pomiędzy organem procesowym i biegłym, a wszystko to w kontekście wpływu na inne czynności procesowe i kształtowanie przebiegu samego postępowania przygotowawczego.

Słowa kluczowe: opinia biegłego, informatyka śledcza, kategoryczność opinii, błędy w opiniowaniu, brak komunikacji z organem procesowym.

Abstract

This paper presents selected cases of irregularities encountered by the author during 20 years of providing expert opinions in criminal cases as a forensic IT expert. It addresses issues related to the storage of opinions and ensuring access to the content transmitted with them as electronically stored information. Furthermore, it raises questions regarding the categorical nature of opinions issued and problems concerning their quality, as well as the lack of communication between the procedural body and the expert – all in the context of the impact on other procedural actions and the shaping of the course of preparatory proceedings.

Keywords: expert opinion, forensic IT, categorical nature of opinions, errors in expert opinions, lack of communication with the procedural body.

(...) Pokazywanie jaki był Pan zawsze nieomylny, a Prokuratura i inne jednostki zawsze złe, też nie było na miejscu. Wylewanie brudów nie powinno mieć miejsca na takim szkoleniu, zamiast tego oczekiwałam informacji praktycznych(...)¹.

Gdy zastanawiałem się nad materiałem podsumowującym moje funkcjonowanie w obszarze usług z zakresu informatyki śledczej, realizowanych na rzecz organów ścigania i instytucji wymiaru sprawiedliwości, najpierw jako biegły sądowy a przez ostatnie 15 lat jako założyciel i prezes zarządu e-Detektywi sp. z o.o., prawie pewnym było, iż skupię się na różnych „ciekawych przypadkach” z jakimi miałem styczność w tym okresie. Przy czym, polemizując z przedstawioną powyżej anonimową oceną prezentacji przedstawionej na XVI edycji Konferencji „Zwalczanie Przestępczości Internetowej” w Sanoku, nigdy moim zamiarem nie było udowadnianie własnej nieomyślności, natomiast nie zgadzam się z zarzutem, iż nie należy pokazywać błędów. Według mnie, publiczne ich pokazywanie i omawianie, nie jest na pewno

¹ Z anonimowych ocen prezentacji: *Cale życie z fuck'upami – 20 lat pracy biegłego. Historia błędów mniejszych lub większych*, Konferencja Zwalczanie Przestępczości Internetowej, edycja XVI, Sanok 2025.

„wylewaniem brudów”, a wręcz przeciwnie – ich prezentowanie, właśnie na przykładach praktycznych, a nie „wydumanej” teorii, może przyczynić się do poprawy jakości usług świadczonych zarówno na rzecz organów ścigania, jak i podniesienia jakości pracy tych ostatnich – a wszyscy zdajemy sobie sprawę z tego, iż nie jest to problem błahy, a wręcz przeciwnie – od działań podejmowanych zarówno przez zlecających jak i wykonawców opinii, niejednokrotnie zależeć mogą dalsze ludzkie losy...

W niniejszej publikacji omówionych zostanie kilka – w mojej ocenie interesujących – przypadków, z jakimi zetknąłem się w trakcie opiniowania. Obejmują one zarówno sytuacje, w których w sposób bardzo specyficzny dokonano interpretacji obowiązujących przepisów prawa w obszarze związanym z opiniowaniem, jak i przypadki, kiedy z różnych przyczyn niezbędne było wykonanie kolejnej opinii w toczącym się postępowaniu.

1. Archiwum opinii i upraszczanie procedur

Pierwszy z omawianych przypadków dotyczył wystąpienia skierowanego do e-Detektywi sp. z o.o. jako wykonawcy ekspertyzy. W przesłanym do spółki piśmie, którego zanonimizowany skan znajduje się poniżej, podmiot wnioskujący zwracał się o udostępnienie ekspertyzy wykonywanej w ramach odrębnego postępowania i dla innego zlecającego.

Wydział _____ pod nadzorem
Prokuratury _____, prowadzi śledztwo, do l.dz. jw. w sprawie przyjmowania, posiadania i przekazywania w nieustalonym czasie, nie wcześniej niż od dnia _____, środków pieniężnych co do których, zachodzi uzasadnione przypuszczenie, że pochodzą z korzyści związanych z popełnieniem czynu zabronionego i działania które mogą udaremnić lub znaczenie utrudnić stwierdzenie ich przestępczego wykrycia tj. o czyn z art. 299 § 1 kk

W toku wykonywanych czynności procesowych ustalono, że na potrzeby postępowania prowadzonego przez Prokuraturę _____ sygn. akt _____ przeciwko _____, wydawali Państwo opinię z zakresu informatyki.

Celem poczynienia stosownych ustaleń na potrzeby niniejszej sprawy, mając na uwadze ekonomikę postępowania i konieczność usprawnienia jego toku, na podstawie art. 15 § 3 kpk zwracam się z uprzejmą prośbą o przekazanie kopii Opinii _____, celem jej służbowego wykorzystania.

Rysunek 1. Pismo przesłane do e-Detektywi sp. z o.o. (po zanonimizowaniu)

Jak można zauważyć na zaprezentowanym dokumencie, podstawą wniosku o udostępnienie opinii był art. 15 par. 3 kpk², który mówi, iż *osoby prawne lub jednostki organizacyjne niemające osobowości prawnej inne niż określone w § 2³, a także osoby fizyczne są obowiązane do udzielenia pomocy na wezwanie organów prowadzących postępowanie karne w zakresie i w terminie przez nie wyznaczonym, jeżeli bez tej pomocy przeprowadzenie czynności procesowej jest niemożliwe albo znacznie utrudnione*. W publikacjach dotyczących tego, wprowadzonego nowelizacją kodeksu karnego z dnia 9 maja 2007 r. (Dz.U. nr 99, poz. 664)

² Ustawa z dnia 6 czerwca 1997 r., *Kodeks postępowania karnego*, tekst jedn. Dz.U. z 2025, poz. 46.

³ Art. 15 § 2 kpk: *Wszystkie instytucje państwowe i samorządowe są obowiązane w zakresie swego działania do udzielania pomocy organom prowadzącym postępowanie karne w terminie wyznaczonym przez te organy.*

paragrafu, w kontekście całego art. 15 kpk, a zwłaszcza różnic pomiędzy paragrafem 2 i 3 wskazuje się, iż gdy organ „żąda” pomocy, to wskazany w tym przepisie podmiot ma obowiązek udzielenia pomocy, natomiast gdy mowa o zwracaniu się o udzielenie pomocy, tego dopowiedzenia brak⁴.

Niezależnie od powyższego, w polskim systemie prawnym, nie ma regulacji nakładających na biegłego lub instytucję specjalistyczną obowiązek archiwizowania i przechowywania przez jakikolwiek okres czasu, wykonanych na zlecenie uprawnionych organów ekspertyz. Nie jest to jedyny problem systemowy w obszarze związanym z wykonywaniem funkcji biegłego sądowego. Wśród znacznie bardziej problematycznych można wskazać, np. brak kontratypu ustawowego związanego z czynnościami biegłego sądowego z zakresu informatyki śledczej w kontekście art. 204 par. 4a kk, jednak jest to już materiał na inne opracowanie. Biegli lub instytucje regulują te kwestie niejako samodzielnie, jednakże brak ujednoliconych rozwiązań wydaje się być w tej sytuacji dość dużym problemem. Kontynuując, należy zauważyć, iż skierowanie tego rodzaju pisma do instytucji specjalistycznej było błędem z dwóch powodów. Po pierwsze, uzyskanie materiałów z innego postępowania przygotowawczego pozostaje w kompetencji Prokuratora i powinno być zrealizowane w oparciu o art. 158 par. 1 kpk, poprzez stosowne wystąpienie do organu prowadzącego postępowanie przygotowawcze, w którym znajduje się ekspertyza, którą chce on uzyskać. Po drugie, wykonanie dyspozycji zawartej w takim piśmie jak zaprezentowane, spowoduje przekazanie informacji, do której zachowania w tajemnicy był zobowiązany podmiot wezwany. Taka czynność, z uwagi na fakt, iż udzielenie pomocy może nastąpić jedynie w granicach prawa, może skutkować odpowiedzialnością karną zarówno po stronie wnioskującego jak i wykonującego dyspozycję zawartą we wniosku. Należy także zauważyć, że przepis ma charakter ogólny, jego literalne brzmienie wskazuje, iż korzystanie z niego przez organ prowadzący postępowanie jest limitowane jedynie brakiem możliwości przeprowadzenia czynności procesowej bez udzielenia pomocy lub jej znacznym utrudnieniem. Zakładając, że przedmiotem obowiązku może być każde zachowanie ułatwiające przeprowadzenie czynności procesowych, o ile są spełnione powyższe warunki, należałoby także przyjąć, że przepis ten legalizuje – działanie w ramach obowiązku prawnego nie może być bezprawne – wkroczenie bez innych ograniczeń w sferę dóbr prawnych, również tych najważniejszych. Regulacja taka, jako nieproporcjonalna i zbyt mało precyzyjna, musiałaby zostać uznana za sprzeczną z Konstytucją. Przyjmując, że wezwanie wystosowane na podstawie tego przepisu nie legalizuje zachowań sprzecznych z innymi przepisami prawa, należy mieć na względzie, że organ władzy publicznej może działać jedynie w granicach i na podstawie prawa (art. 7 Konstytucji). W tym kontekście wzywanie do zachowań nielegalnych i korzystanie z ich owoców byłoby rażąco sprzeczne z zasadą demokratycznego państwa prawnego, a jeżeli zachowanie bezprawne realizowałoby przedmiotowe znamiona czynu zabronionego, takie wezwanie stanowiłoby przekroczenie prawnokarnej normy zakazującej podżegania do przestępstwa⁵. Nie powinien więc dziwić fakt, iż do organu wnioskującego została przekazana informacja o niemożności wykonania przez instytucję specjalistyczną wnioskowanych czynności.

⁴ Andrzej Jezusek, *Niektóre aspekty powszechnego obowiązku udzielenia pomocy organom prowadzącym postępowanie karne*, [w:] *Palestra* 6/2016 s. 41.

⁵ Andrzej Jezusek, *Niektóre aspekty...* s. 44.

2. Instytucja specjalistyczna jako drukarnia

Z nieco odmienną sytuacją mieliśmy do czynienia w kolejnym z omawianych przypadków, w którym Sąd skierował wystąpienie związane z koniecznością wydrukowania przez instytucję specjalistyczną części materiałów dostarczonych wraz z opinią jako załącznik elektroniczny. Przywiązanie do formatu papierowego, jak również nacisk kładziony na wydruki danych, może wynikać z przypadków niezrozumienia faktu, z jaką ilością informacji możemy mieć do czynienia w przypadku średnio skomplikowanego urządzenia elektronicznego. Jako drugi, nieco żartobliwy powód, możemy wskazać na pokutujące w społeczeństwie przekonanie, iż waga sprawy oraz powaga Sądu rośnie wprost proporcjonalnie od ilości tomów akt, które zarejestrują kamery stacji telewizyjnych na stole sędziowskim. Bezspornym natomiast pozostaje fakt, iż w przypadku niektórych środków dowodowych (w tym niektórych opinii) wiodącą formą ich prezentacji pozostaje forma papierowa⁶, jednak w omawianym przypadku nie miało to zastosowania. W tej konkretnej sprawie, wykonanie opinii obejmowało jedynie akwizycję, czyli zgromadzenie i przygotowanie do dalszej analizy i interpretacji, danych zawartych w pamięci cyfrowego nośnika informacji. Z uwagi na dużą liczbę danych, materiały wyjściowe dostarczone zostały na pendrive, wraz z narzędziem umożliwiającym przeglądanie, przeszukiwanie i ewentualne wyodrębnianie do dalszych raportów istotnych treści. Takie działanie jest w przypadku badań wykonywanych przez spółkę regułą, ponieważ umożliwia dalsze swobodne przetwarzanie dostarczonych danych. Wykonana opinia nie obejmowała żadnej formy analizy i oceny przydatności przez biegłego ujawnionego materiału, stąd też zdziwienie wywołał fakt zwrócenia się do instytucji z wnioskiem o wydrukowanie części zabezpieczonych danych. Ponieważ zlecający wyraził zgodę na koszty przedstawione przez instytucję specjalistyczną, przedmiotowy materiał został wydrukowany we wskazanym zakresie, czego wynikiem było ponad 600 stron formatu A4 zawierających różnego rodzaju konwersację. Abstrahując od kwestii ograniczonej przydatności tego rodzaju treści – brak możliwości jakiegokolwiek efektywnego jej przeszukiwania i analizowania – zdziwienie może budzić fakt zlecenia tej czynności do podmiotu wykonyującego opinię, zamiast wykonanie jej – po wcześniejszej analizie jej niezbędności i zasadności – we własnym zakresie, zwłaszcza w sytuacji, w której obsługa urządzeń peryferyjnych komputera nie stanowi wiadomości specjalnych, o których mowa w art. 193 par. 1 kpk⁷. Także aspekt ekonomiczny nie znajduje w tej sytuacji jakiegokolwiek uzasadnienia.

3. Nieuzasadniona kategoryczność opinii

W wielu przypadkach, na przestrzeni lat, zlecano nam ekspertyzy, które stanowiły pewnego rodzaju mechanizm weryfikacji czynności przeprowadzanych wcześniej przez innych biegłych. Nie były to sytuacje, w których kwestionowano by ich rzetelność czy profesjonalizm, a raczej pewien sposób upewnienia się, iż w toku postępowania przygotowawczego zostało wykonane wszystko co było możliwe w zakresie badań dowodów cyfrowych. W wielu przypadkach, zapoznając się z przekazanymi materiałami, napotykałszy na treści formułowane jako kategoryczne, bez racjonalnych powodów. A przecież już ponad sto lat temu Edmond Locard

⁶ Wojciech Pilszak, *Informacje przechowywane elektronicznie a opinia z informatyki śledczej*, [w:] Cybersecurity & Cybercrime Tom: 1, Nr: 8 – Numer specjalny, 2025, s. 170.

⁷ Ustawa z dnia 6 czerwca 1997 r., *Kodeks postępowania karnego*, tekst jedn. Dz.U. z 2025, poz. 46.

pisał „Najbardziej niebezpiecznymi pomocnikami wymiaru sprawiedliwości są tego rodzaju biegli, którzy swoje odkrycia lub orzeczenia uważają za nienaruszalne świętości (...). Najbardziej niebezpieczny jest jednak biegły, który powziąwszy w swym życiu jedną jedyną ideę, pielęgnuje ją jak najdroższą dziecinę – poświęci dla niej wszystko. Timeo virum unius concepti”⁸. Należy zauważyć, iż informatyka śledcza jako młoda dziedzina nauk sądowych podlega ciągłym zmianom, które są wymuszane poprzez rozwój technologii. Do kwestii tej powrócimy ponownie w dalszej części niniejszego opracowania. W tej chwili ograniczymy się tylko do dygresji, iż w przypadku opinii z zakresu informatyki śledczej, do wyników badań formułowanych w postaci stanowiska kategorycznego, należy podchodzić z dużą ostrożnością. W prezentowanych poniżej przykładach, jak można się przekonać, tej ostrożności zabrakło:

W toku przeprowadzonej analizy nie ujawniono w środowisku systemowym urządzenia instalacji aplikacji klienckich serwisów randkowych. Wobec tego pozyskanie danych autoryzacyjnych umożliwiających logowanie do któregośkolwiek z tego typu serwisów nie było możliwe.

Rysunek 2. Przykład kategorycznego formułowania wniosków do opinii

w celu dalszego	
przejęcia do serwisu randkowego koniecznym jest zalogowanie się poprzez podanie adresu	
poczty internetowej „Email” oraz hasła. Przy użyciu innych aplikacji znajdujących się	
pamięci telefonu ustalono używany email	W systemie nie jest
zapamiętane hasło do zalogowania się w serwisie	Nie ma możliwości zalogowania
się do serwisu.	
W celu uzyskania danych umożliwiających zalogowanie się do serwisu	wykonano
dodatkowo ekstrakcję pamięci telefonu przy użyciu programu	
Utworzono raport pamięci telefonu, który dokładnie przeanalizowano. Nie znajdują się w nim	
jakośkolwiek informacje umożliwiających zalogowanie się do serwisu randkowego.	

Rysunek 3. Kolejny (zanonimizowany) przykład wniosków kategorycznych

Zarówno w pierwszym, jak i drugim przykładzie, autorzy opinii wykazali się bardzo dużą pewnością co do uzyskanych wyników, stwierdzając kategorycznie, iż w poddanych badaniu urządzeniach nie ma poszukiwanych informacji. Kolejna ekspertyza wykazała jednak coś całkowicie przeciwnego i pozwoliła na uzyskanie informacji poszukiwanych przez zlecającego. Nie należy jednak wyciągać pochopnych wniosków co do jakości i rzetelności przeprowadzonych badań – obie ekspertyzy – w mojej ocenie – zostały wykonane zgodnie ze sztuką, jednak ich autorzy zastosowali nieco odmienne podejście. Gdyby w sporządzanych przez siebie wnioskach zawarli sformułowanie, iż „zastosowane metody oraz narzędzia jakimi dysponował biegły na dzień wykonywania opinii nie dostarczyły informacji pozwalających na zalogowanie się do wskazanego serwisu” sytuacja byłaby jednoznaczna. Podobnie wygląda sytuacja, kiedy biegłemu nie udaje się przełamać zabezpieczenia urządzenia, lub pozyskać z niego określonych danych. Stosowanie zapisów, iż coś jest „niemożliwe do zrobienia” może, w przeważającej mierze w sposób niezamierzony, wprowadzać odbiorcę w błąd co do generalnych możliwości

⁸ Edmond Locard, *Dochodzenie przestępstw według metod naukowych*, tłum. R. Merson, E. Wiśniewski, Warszawa 1937, s. 252–253.

technicznych. Oczywiście, w niektórych przypadkach jest to bardzo wygodne dla zlecającego, który otrzymuje w ten sposób doskonale usprawiedliwienie, pozwalające mu nie kontynuować dalej określonych czynności. Należy przypuszczać, iż żaden biegły nie jest tak pewien swoich umiejętności oraz możliwości rozwiązań, którymi dysponuje, aby z premedytacją używać tak kategoriycznych sformułowań. Zdecydowanie bardziej na miejscu jest stwierdzenie, iż „*na dzień wykonania opinii oraz przy wykorzystaniu zasobów programowych i sprzętowych pozostających w dyspozycji biegłego, nie było możliwości osiągnięcia określonych rezultatów*”. Natomiast użycie stwierdzeń kategoriycznych, może wywołać u niektórych odbiorców wrażenie braku profesjonalizmu wykonawcy opinii.

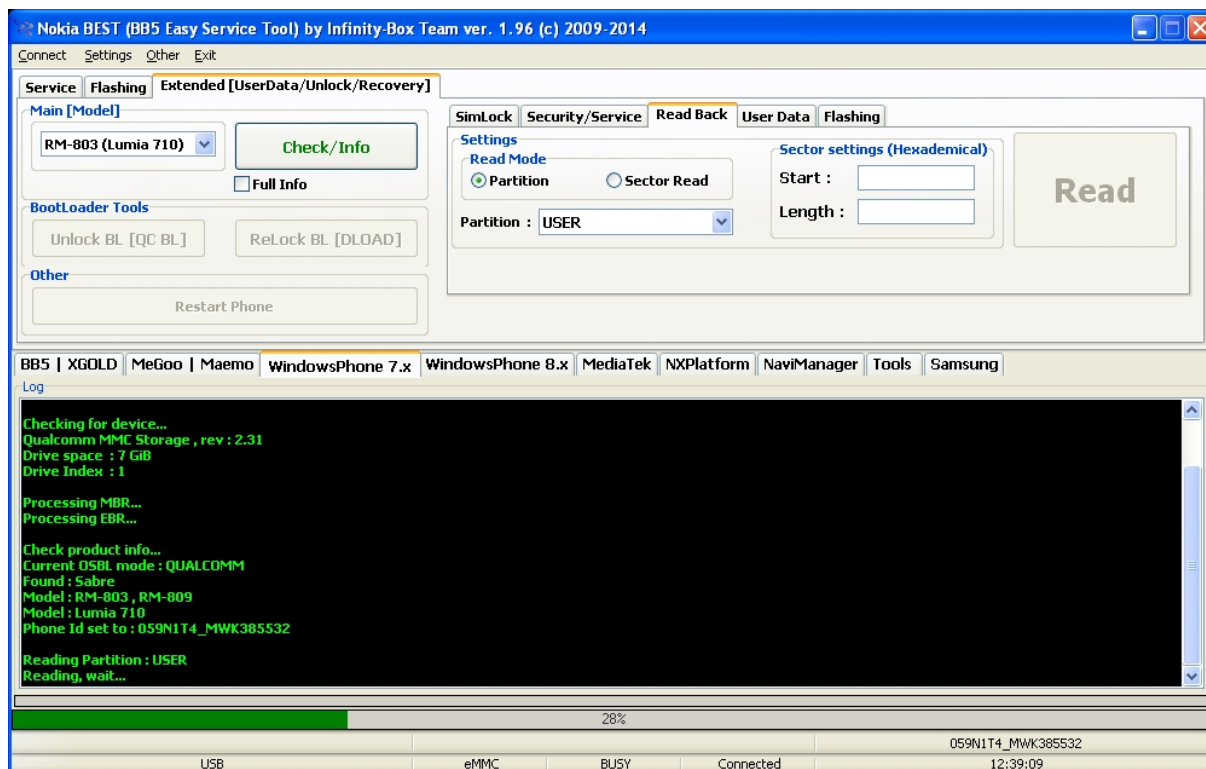
4. Mit kopii binarnej

W kolejnym z przypadków badaniu poddawany był także telefon komórkowy, jednakże była to sytuacja odmienna od poprzedniej. Zanim jednak przejdziemy do szczegółowego opisu, kilka słów wprowadzenia.

W początkowych latach rozwoju informatyki śledczej, kopia binarna stanowiła pewnego rodzaju wzór, do którego dążyli wszyscy specjaliści zabezpieczający dane cyfrowe. Było to spowodowane stanem rozwoju technologii i możliwościami badawczymi, w ówczesnym okresie skupiającymi się, przede wszystkim, na tzw. badaniach *post mortem*, czyli analizie kopii binarnej i zastanego na niej stanu danych. Przypomnijmy, iż kryminalistyczna kopia binarna to odpowiednio uwierzytelniona kopia nośnika dowodowego, wykonana na inny nośnik lub do pliku, zawierająca identyczny układ wszystkich danych (zer i jedynek) jak na materiale źródłowym, której proces wykonania został odpowiednio udokumentowany. Wraz z postępem technologicznym zaczęły pojawiać się rozwiązania, które w znacznym stopniu uniemożliwiały jej wykonanie, wymuszając zastosowanie innych rozwiązań pozwalających na zabezpieczenie jak najpełniejszego zbioru danych. Nie da się jednak zaprzeczyć, iż do dnia dzisiejszego stanowi ona najbardziej kompletne źródło informacji o zabezpieczanym nośniku, i tam, gdzie jest to tylko możliwe, jest sporządzana nadal.

Jednakże kompletność zabezpieczonych danych, to nie to samo, co prawidłowe ich zdekodowanie i dostęp do nich. Niejednokrotnie zastosowane narzędzia umożliwiają przeprowadzenie procesu wykonania kopii binarnej, ale mają problemy z prawidłowym zdekodowaniem wszystkich danych. Informacje te, w wielu przypadkach, są zawarte w dokumentacji. Jednak bardzo często zdarza się, że badacze – szczególnie ci początkujący – ufają bezgranicznie możliwościom oferowanym przez narzędzia, co może prowadzić do pominięcia kluczowych danych. Co więcej, w materiałach szkoleniowych zetknęliśmy się z zaleceniami dotyczącymi akwizycji danych z telefonu komórkowego, aby – jeśli udało się poprawnie wykonać kopię binarną – nie uruchamiać go, nawet w celu zweryfikowania, jakiego rodzaju dane zostały zdekodowane i jakie jest przełożenie tych informacji na te widoczne w urządzeniu.

W opisywanym przypadku do wykonania kopii binarnej niezaszyfrowanej pamięci telefonu zostało wykorzystane rozwiązanie serwisowe *Infinity BB5 Easy Service Tool*, z którego przykładowy zrzut ekranu został zaprezentowany poniżej.



Rysunek 4. Zrzut ekranu z aplikacji Infinity BB5 Easy Service Tool

Dla modelu poddanego badaniom w ramach ekspertyzy, rozwiązanie serwisowe – pomimo wykonania prawidłowej kopii binarnej – nie parsowało poprawnie plików graficznych, co spowodowało, iż szereg kluczowych dla postępowania informacji nie był dostępny dla zlecającego. Niestety, biegły wykonujący ekspertyzę – przekonany o kompletności kopii binarnej – nie porównał, nawet ogólnie, zawartości urządzenia z wynikami uzyskanymi w trakcie odczytu, co doprowadziło do pominięcia kluczowych dla postępowania informacji. Dopiero kolejna ekspertyza wykonana przy zastosowaniu innych rozwiązań, oraz kompleksowa weryfikacja uzyskanych wyników doprowadziły do zabezpieczenia istotnych treści.

Podsumowując ten przypadek, należy szczególnie uwypuklić znaczenie weryfikacji informacji rozpoznanych przez wykorzystywane do odczytu narzędzie, z tymi dostępnymi w urządzeniu. Niezależnie od zastosowanej metody akwizycji i wykorzystywanych rozwiązań, nikt nie zagwarantuje nam kompletności zdekodowanych informacji, także przy kompletnym odczycie danych. Nawet, jeżeli akwizycja obejmie wykonanie kopii binarnej, to ograniczenia różnorodnych, wykorzystywanych szczególnie w informatyce śledczej urządzeń mobilnych rozwiązań, wymuszają stosowanie zasady ograniczonego zaufania w stosunku do przekształconych w informacje zdekodowanych danych i bezwzględne porównywanie ich, nawet na poziomie ogólnym, z tymi dostępnymi w urządzeniu. Oczywiście jest, iż w wielu sytuacjach, możliwości przeprowadzenia tego rodzaju porównań będą ograniczone, zwłaszcza w przypadkach, kiedy agregowane są dane pozostające w obszarze pamięci niedostępnym dla użytkownika urządzenia, ale zignorowanie tego etapu badań może prowadzić do zawężenia uzyskanych wyników, a w najgorszym przypadku do pominięcia istotnych dowodów.

Wszystko przez wirusa

Z odmienną sytuacją mieliśmy do czynienia w tym przypadku, w którym w przeciwieństwie do powyżej opisywanej sytuacji, dostęp do informacji nie był ograniczony przez wykorzystane narzędzia, a jedynie wiedzę wykonującego ekspertyzę. Problem dotyczył komunikatora Gadu-Gadu w wersji 10, czyli rozwiązania archaicznego, nawet w momencie wykonywanych kilka lat temu badań. Jednak w okresie kiedy wykonywano opinię pierwotną, rozwiązanie to było w Polsce bardzo popularne, a dokumentacja opisująca jego parametry powszechnie dostępna. W chwili pojawienia się wersji 10, na oficjalnej stronie komunikatora można było przeczytać, iż *jest to najpopularniejszy komunikator internetowy w Polsce. Łącznie miesięcznie przez GG rozmawia 10 mln osób. Program jest łatwy w obsłudze i przystępny, zarówno dla początkujących internautów, jak i dla zaawansowanych miłośników Internetu. Gadu-Gadu coraz częściej służy do komunikacji w pracy, w szkole, jak i administracji. Specjalne numery GG posiadają liczne instytucje, osobistości, jak i redakcje popularnych mediów*⁹. Wydawać by się mogło, iż wiedza o możliwości szyfrowania archiwum komunikatora, powinna być wiedzą powszechną, szczególnie wśród zajmujących się tą problematyką informatyków śledczych, ale jak okazało się w trakcie badań, były to tylko optymistyczne założenia.

Informację o szyfrowaniu archiwum komunikatora, możemy znaleźć w pliku konfiguracyjnym *ProfileBasic.xml*, który znajduje się w folderze o nazwie odpowiadającej numerowi UID użytkownika. Dla komunikatora zainstalowanego na dysku twardym C: komputera i UID użytkownika komunikatora: 77879835, lokalizacja ta może wyglądać np. tak:

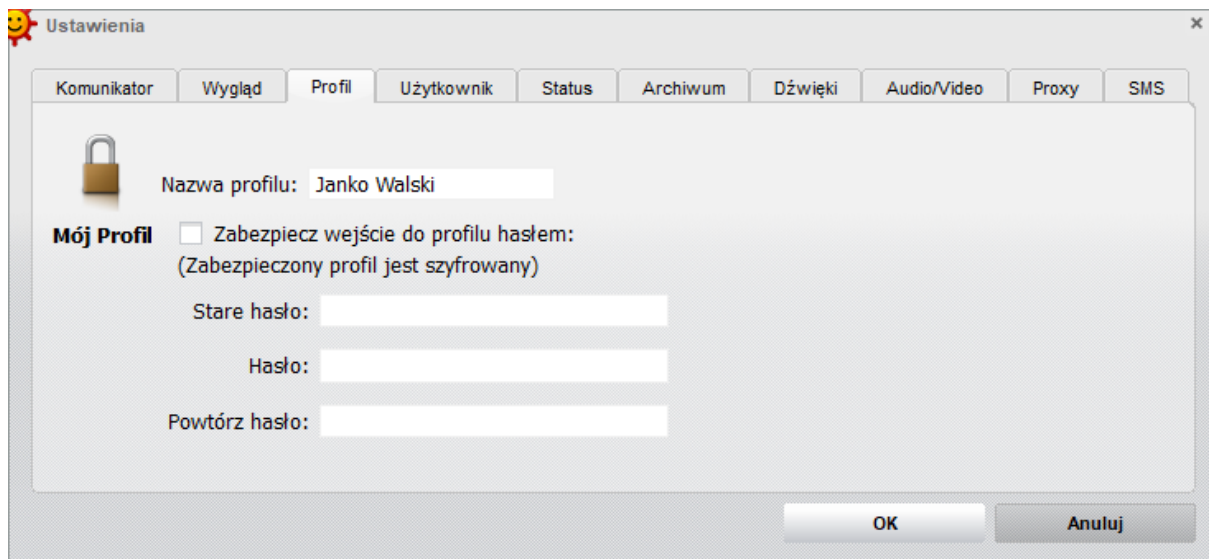
C:\Users\XXX\AppData\Roaming\Gadu-Gadu 10\77879835

Poniżej przedstawiono wygląd pliku konfiguracyjnego *ProfileBasic.xml*:

```
<ProfileBasic>
  <UID>77879835</UID>
  <Name>Janko Walski</Name>
  <AutoStart>true</AutoStart>
  <SkinName>GG10</SkinName>
  <ContactListVersion>4</ContactListVersion>
  <CurrentAvatar>0</CurrentAvatar>
  <IsEncrypted>true</IsEncrypted>
  <ProfilePasswordHash>gnuLUuqKcXxMNZFokbaOew==</ProfilePasswordHash>
    <ContactWindowRect x="1012" y="51" width="611" height="812">
    </ContactWindowRect>
  <loadedApplicationID>id0</loadedApplicationID>
</ProfileBasic>
```

Treść istotną w tym konkretnym przypadku zaznaczono kolorem czerwonym, a powiązane ustawienia szyfrowania w samym komunikatorze znajdują się w widocznej poniżej zakładce. Ustanowienie hasła powoduje zaszyfrowanie profilu, w tym także informacji znajdujących się w archiwum, przechowywanym lokalnie.

⁹ <https://biuroprasowe.gg.pl/specjalny-numer-gg-dla-unii-europejskiej/> – ostatni dostęp 17.11.2025 r.



Rysunek 5. Wygląd zakładki [Profil] komunikatora Gadu-Gadu 10

Jak można zauważyć, na podstawie przedstawionych danych, stwierdzenie faktu zaszyfrowania archiwum wydaje się nie być szczególnie trudne. Tym bardziej dziwić może zawarte w pierwotnej ekspertyzie stanowisko biegłego, iż „archiwum jest prawdopodobnie uszkodzone przez wirusa” zwłaszcza, że stanowiło ono konstatację, która nie została poparta jakimikolwiek innymi dowodami, którymi mogłyby być np. logi z programu antywirusowego. Badania przeprowadzone w ramach kolejnej opinii, zdecydowanie zaprzeczyły prezentowanemu twierdzeniu i pozwoliły na odczytanie zaszyfrowanego archiwum. Bez odpowiedzi pozostaje pytanie, na ile działania podjęte przez biegłego w ramach pierwszej opinii były spowodowane jego ignorancją i niewiedzą, a ile w nich było lekceważenia dla postępowania, w ramach którego zdecydowano się skorzystać z jego wiadomości specjalnych. Na marginesie dodać należy, iż przedmiotowa sprawa nie dotyczyła błahostki, a wręcz przeciwnie – jej ciężar gatunkowy był znaczny...

6. Uszkodzony pendrive

Kolejna opisywana sytuacja stanowi znakomity przykład tego, iż dostarczane opinie nie powinny – jak mówi się w żargonie procesowym – „zalegać” w aktach, a ich zawartość powinna być poddawana bez zbędnej zwłoki analizie, w celu wykorzystania zgromadzonych informacji w toku dalszego postępowania przygotowawczego. Należy pamiętać, iż w przypadku dowodów cyfrowych, retencja danych może stanowić największe wyzwanie, a jednocześnie przeszkodę w osiągnięciu sukcesu. Bezzwłoczne działanie jest uzasadnione także z innych powodów – szybkie zapoznanie się z przekazaną opinią oraz z załącznikami do niej, pozwala na ujawnienie ewentualnych problemów technicznych spowodowanych np. uszkodzeniem nośnika stanowiącego załącznik do ekspertyzy, a zawierającego informacje odczytane z badanego urządzenia. W prezentowanej sytuacji, załącznikami znajdującymi się na nośniku dołączonym do przygotowanej opinii zainteresował się dopiero obrońca oskarżonego, podczas przewodu sądowego. Z materiałem tym nie zapoznano się podczas całego trwania postępowania przygotowawczego, chociaż hipotetycznie założyć można, iż zgromadzone informacje mogły przyczynić się zarówno do wzmocnienia dowodów zgromadzonych zarówno po stronie oskarżenia jak i obrony. Dopiero działania podjęte przez obrońcę spowodowały ujawnienie uszkodzenia nośnika i miało to miejsce ponad 18 miesięcy od dostarczenia ekspertyzy. Jak już wspomniano wcześniej,

w Polsce żadne normy prawne nie obligują do przechowywania sporządzonych opinii przez biegłego czy też instytucję specjalistyczną – jest to tylko i wyłącznie ich dobra wola. W omawianym przypadku możliwe było odtworzenie z repozytorium instytucji specjalistycznej zawartości dołączonego nośnika, co pozwoliło uniknąć konieczności przeprowadzenia ponownych badań materiału dowodowego. Należy zaznaczyć, iż w każdym przypadku, do opinii przygotowywanej w laboratorium e-Detektywi sp. z o.o., dołączana jest informacja jak przedstawiona poniżej, która informuje zlecającego o konieczności zachowania pewnych procedur, dających zwiększoną gwarancję ochrony przechowywanych danych przed ich utratą lub zniszczeniem. Kwestią otwartą pozostaje fakt, czy podmiot zlecający opinię do tych wskazówek się zastosuje...

7. Informacje dodatkowe

1. Niniejszy dokument stanowi realizację dyspozycji zawartej w art. 200 Ustawy Kodeks Postępowania Karnego.
2. Integralnym elementem niniejszej opinii, zawierającym wskazane w części opisowej dane, które mogą podlegać wykorzystaniu w ramach dalszych czynności, w szczególności dodatkowych badań i analiz, jest dołączony cyfrowy nośnik danych o nazwie "OPINIA".
3. W celu zapoznania się z danymi znajdującymi się na nośniku zalecany jest skopiowanie jego zawartości (z uwzględnieniem ukrytego katalogu o nazwie ZL) na dysk lokalny komputera, a następnie należy otworzyć, w przeglądarce WWW (Google Chrome, Opera lub Microsoft Edge), skopiowany plik [index.html](#) pochodzący z katalogu głównego dołączonego nośnika.
4. Bezpośrednio z modułu interaktywnej opinii, z poziomu przeglądarki internetowej, istnieje możliwość zapoznania się z jej treścią, nawigowania po sekcjach oraz wydrukowania dowolnego fragmentu.
5. Informacje dołączone na cyfrowym nośniku danych o nazwie "OPINIA" zostały po ich zapisaniu zweryfikowane pod kątem poprawności. Aby ograniczyć możliwość ich utraty lub uszkodzenia, zalecane jest wykonanie kopii przekazanego nośnika i przechowywanie go niezależnie od nośnika będącego integralnym elementem opinii.

Rysunek 6. Informacje o zalecanych procedurach bezpieczeństwa umieszczane w ekspertyzie

Opisywaną sytuację można też przedstawić z innego punktu widzenia – to laboratorium powinno dołożyć należytej staranności, aby zapewnić maksymalne bezpieczeństwo przekazywanych danych. Takie stanowisko można by nawet uznać za słuszne, gdyby nie realia, w których funkcjonują wszyscy biegli wykonujący zlecenia na rzecz organów ścigania. W rzeczywistości tej, w przeważającej większości przypadków, głównym kryterium decydującym o atrakcyjności wykonawcy jest cena. Zrozumiałym jest, iż sporządzenie dodatkowej kopii bezpieczeństwa danych podnosi koszt wykonania opinii, a tym samym zmniejsza atrakcyjność potencjalnego zleceniobiorcy. Nikt zaś w warunkach rynkowych nie będzie sam świadomie ograniczał swojej konkurencyjności, stąd zdecydowanie prostszym rozwiązaniem jest umieszczenie informacji o konieczności wykonania kopii bezpieczeństwa danych przez zlecającego opinię, niż inwestowanie pieniędzy i poświęcanie czasu na jej wykonanie.

7. Problemy z komunikacją

W przygotowywanych na potrzeby różnych grup docelowych szkoleniach, wielokrotnie poruszany jest temat komunikacji pomiędzy organem procesowym zlecającym ekspertyzę a podmiotem ją wykonującym. Wskazywana jest istotna rola dwukierunkowego przepływu

informacji, która przekłada się na ostateczną przydatność przygotowywanej ekspertyzy w postępowaniu. Niestety, znacznie częściej jest jednak tak, iż komunikacja realizowana jest w formie szczątkowej, a do rzadkości wcale nie należą sytuacje, w których nie występuje ona wcale. Tak też wyglądało to w opisywanym przypadku.

Do badań został przesłany materiał dowodowy w postaci telefonu komórkowego. Fakt, iż jest on zablokowany hasłem, które nie zostało przekazane, został stwierdzony podczas ewidencjonowania dowodu w systemie administracyjnym laboratorium. Niezwłocznie poinformowano o tym fakcie zlecającego, przekazując także informacje o potencjalnych możliwościach technicznych i przewidywanych kosztach przełamania zabezpieczenia. W oczekiwaniu na decyzję zlecającego, ograniczono się do podstawowych czynności badawczych, w tym działań identyfikujących zastosowane zabezpieczenie, oraz wykonania dokumentacji fotograficznej urządzenia. Jest to standardowa procedura, która pozwala na przygotowanie do ewentualnych dalszych badań, a jednocześnie nie powoduje ponoszenia przez zleceniobiorcę istotnych wydatków, jeśli kosztorys nie zostanie zaakceptowany. W tym jednak wypadku, decyzji dotyczącej kosztów nie otrzymano, natomiast do laboratorium, z chwilą upływu terminu na wydanie opinii wskazanego w postanowieniu, wpłynęło pismo z pytaniem o stan badań urządzenia. Po przekazaniu informacji, iż zlecający nie ustosunkował się do przekazanego kosztorysu, a co z tego wynika, wykonane zostały jedynie czynności wstępne, zakładano, iż niezwłocznie zostanie przekazana oczekiwana informacja. Zamiast niej otrzymano postanowienie o uchyleniu wydanego postanowienia o dopuszczeniu dowodu z opinii instytucji specjalistycznej, co spowodowało zakończenie badań.

Przedstawiona sytuacja stanowi wręcz podręcznikowy przykład braku komunikacji ze strony organu zlecającego badania z biegłym. Można by nawet zaryzykować twierdzenie, iż jest to milczenie organu, znane z postępowania administracyjnego, lecz przeniesione na grunt procedury karnej, jednak dużo bardziej interesujące wydają się rozważania na temat samego procesu skorzystania z pomocy instytucji specjalistycznej. Zgodnie z art. 193 par. 1 kpk, *jeżeli stwierdzenie okoliczności mających istotne znaczenie dla rozstrzygnięcia sprawy wymaga wiadomości specjalnych, zasięga się opinii biegłego albo biegłych*¹⁰. Kluczowym dla dalszych rozważań jest „*stwierdzenie okoliczności mających istotne znaczenie dla rozstrzygnięcia sprawy*”. W opisywanym przypadku, teoretycznie, mogliśmy mieć do czynienia z sytuacją, kiedy na skutek innych czynności procesowych, w tym zgromadzenia innych dowodów, informacje zawarte w pamięci przekazanego do badań urządzenia nie miały już istotnego znaczenia dla rozstrzygnięcia sprawy. Przy czym należy pamiętać, iż zlecający nie miał możliwości w żaden sposób ocenić wagi tych informacji i stopnia ich wpływu na prowadzone postępowanie, ponieważ z uwagi na brak dostępu do urządzenia (nieznajomość hasła) nie mógł się z nimi zapoznać. Z tego powodu hipotezę o utracie znaczenia informacji znajdujących się w urządzeniu, dla prowadzonego postępowania, należałoby uznać za chybioną. Drugim argumentem przemawiającym za wątpliwym prawdopodobieństwem rozważanej utraty istotnej wartości dowodowej, jest brak jakiegokolwiek informacji na ten temat w uzasadnieniu postanowienia uchylającego badania. Logicznym wydaje się twierdzenie, iż fakt ustania konieczności stwierdzenia okoliczności mających istotne znaczenie dla rozstrzygnięcia sprawy, powinien zostać wskazany w uzasadnieniu postanowienia. Przy czym wystarczyłoby wyłącznie stwierdzenie ogólne –

¹⁰ Ustawa z dnia 6 czerwca 1997 r. *Kodeks postępowania karnego*.

brak jest jakichkolwiek przesłanek, aby wprowadzać biegłego w szczegółowe okoliczności postępowania. W uzasadnieniu przekazanego postanowienia tego rodzaju informacji nie zawarto, ograniczono się jedynie do wskazania faktu niedotrzymania terminu wykonania badań, co było co najmniej dziwne w kontekście całkowitego braku komunikacji organu procesowego z biegłym, w tak istotnych kwestiach jakimi jest dostarczenie posiadanego kodu zabezpieczającego, czy też akceptacja wstępnych kosztów wykonania opinii. Jak zatem można zauważyć, brak prawidłowej komunikacji może w pewnych sytuacjach prowadzić nawet do pojawienia się uzasadnionych wątpliwości co do prawidłowej realizacji celów postępowania karnego¹¹ a nawet podejrzeń o naruszenie zasady obiektywizmu¹². Czy wątpliwości te znajdują swoje potwierdzenie, zależy od wielu innych czynników, indywidualnych dla każdego postępowania, jednakże sytuacje, jak opisywana powyżej, na pewno nie przyczyniają się do ich wyjaśnienia.

Podsumowanie

Ponownie należy zdecydowanie podkreślić, iż niniejsza publikacja nie ma na celu piętnowania jakichkolwiek osób czy też instytucji, wszak *errare humanum est*¹³. Nie możemy jednak dopuścić do tego, aby w myśl źle rozumianej solidarności branżowej czy zawodowej przechodzić do porządku dziennego nad ewidentnymi przypadkami błędnych działań, licząc na to, iż pozostaną one niezauważone. Nikt z nas nie chciałby, aby w ważnej dla niego sprawie została wydana nierzetelna opinia, albo pominięto kluczowe dowody. Każdy człowiek popełnia błędy, ale nauka opiera się także na ich analizie i wyciąganiu wniosków na przyszłość, które pozwolą je ograniczyć lub wyeliminować. Niezależnie od tego czy analizujemy jedynie małe niedociągnięcie, czy też ogromną pomyłkę, wnioski wyciągnięte z naszych działań mogą w przyszłości posłużyć jako podstawa do poprawy jakości naszej pracy czy też zwiększenia profesjonalizmu oferowanych usług.

Literatura

1. Ustawa z dnia 6 czerwca 1997 r., Kodeks postępowania karnego, tekst jedn. Dz.U. z 2025, poz. 46.
2. Andrzej Jezusek, Niektóre aspekty powszechnego obowiązku udzielenia pomocy organom prowadzącym postępowanie karne, [w:] Palestra 6/2016.
3. Edmond Locard, Dochodzenie przestępstw według metod naukowych, tłum. R. Merson, E. Wiśniewski, Warszawa 1937, s. 252-253.
4. Wojciech Pilszak, Informacje przechowywane elektronicznie a opinia z informatyki śledczej, [w:] Cybersecurity & Cybercrime Tom: 1, Nr: 8 – Numer specjalny, 2025.

Źródła internetowe

1. <https://biuroprasowe.gg.pl/specjalny-numer-gg-dla-unii-europejskiej/> – ostatni dostęp 17.11.2025 r.

¹¹ Art. 2 Ustawy z dnia 6 czerwca 1997 r. *Kodeks postępowania karnego*.

¹² Tamże, Art. 4.

¹³ Autorstwo powiedzenia *Errare humanum est* (błądzić jest rzeczą ludzką) przypisuje się Cynceronowi, który użył go w swojej pracy „De natura deorum”.

Analiza nagłówków poczty elektronicznej. Przegląd metod i wybranych narzędzi wspomagających analizę

Każdy samodzielnie może przeprowadzić pełną analizę wiadomości pocztowej. Najważniejszym oczywiście poza treścią wiadomości – elementem e-maila są nagłówki. Można z nich odczytać drogę, jaką przebyła wiadomość, zanim dotarła do naszej skrzynki, a także: jakiego programu użył adresat, wysyłając ten list, a nawet to, czy przesyłka została sprawdzona np. przez program antywirusowy.

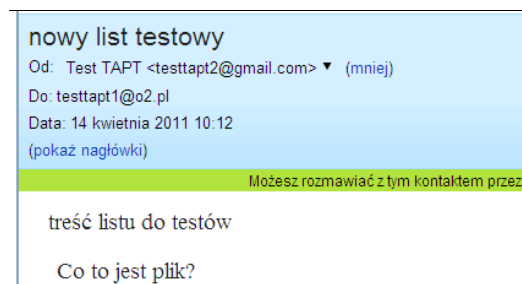
Analiza nagłówków poczty elektronicznej (tzw. *email header analysis*) to podstawowa technika w **informatyce śledczej** i cyberbezpieczeństwie – pozwala ustalić źródło wiadomości, trasę przesyłania, użyte serwery, a czasem też ujawnia fałszerstwa (*spoofing*).

Poniżej postaram się przybliżyć łatwy sposób do zidentyfikowania nieznanego nadawcy listu, bo przecież w każdym z nas drzemie ciekawość, chcemy wiedzieć czy nasz adres został wybrany przypadkowo, polecony przez kogoś, czy też skradziony z jakiejś bazy danych. Dzięki prezentowanemu programowi jesteśmy w stanie sprawdzić skąd został nadany list i jaką drogę przebył zanim trafił do naszej skrzynki e-mailowej. Program może być aktywnie wykorzystywany do śledzenia wykroczeń i przestępstw w cyberprzestrzeni. Raporty automatycznie wygenerowane przez program (zapisane w formie elektronicznej bądź też wydrukowane) mogą stanowić materiał dowodowy.

Informacje praktyczne:

- Nazwa użytkownika najczęściej nie jest imieniem i nazwiskiem adresata, jest to dowolna nazwa wybrana przez użytkownika, lecz najczęściej ograniczona względami technicznymi zawierająca 7–14 znaków alfanumerycznych, różnych od znaków specjalnych i przeważnie pisana małymi literami. Przykłady: bolekkowalski@firma.pl., bolekm@sanok.com.
- Wielkość przesyłanych listów elektronicznych może być ograniczona przez dostawcę Internetu, z którego usług korzysta użytkownik, do określonej pojemności na dysku serwera, na którym są składowane przesyłane informacje (najczęściej to zakres 500kB, 5MB, spotykane są skrzynki, których załączniki do wiadomości mogą sięgać 100MB czy 500 MB a sama pojemność skrzynki to nawet 10GB i więcej).
- Dla osób, które z różnych przyczyn nie mogą zainstalować programu do obsługi poczty lub sprawdzając pocztę korzystają z kilku komputerów (np. na uczelni, z dostępnego Hot-Spot itd., czy różnych urządzeń – telefon komórkowy, tablet czy komputer...) polecane są konta, które można sprawdzać z poziomu strony WWW (bezpośrednio na serwerze, na którym jest skrzynka pocztowa, wszystkie popularne portale oferują taką usługę). Obsługa takiego konta jest bardzo prosta nawet dla niedoświadczonego użytkownika.
- W przypadku, gdy adres e-mail jest zbyt długi, np. bolekm.kowalski@turystyka.sanok.pl, wielocłonowy, trudny do zapamiętania, wykorzystuje się usługę – tzw. „alias” – wysyłając pocztę na nowy – „krótszy” – adres, list trafi na stary adres (bez potrzeby zmiany konfiguracji programów pocztowych).

¹ Marek Stawarczyk – biegły sądowy Sądu Okręgowego w Krośnie z zakresu informatyki oraz informatyki śledczej.



Rys. 1. Standardowy nagłówek listu (otwarcie skrzynki przez stronę WWW)

Nagłówki jawne – część jawna, czyli to, co widzi i wypełnia „zwykły Kowalski” niezależnie od narzędzia, jakie zostało użyte do wyprodukowania, wysłania, odbioru i przeczytania listu-wiadomości.

- **From/ Od** – nadawca,
- **To/ Do** – tu należy wpisać adresata lub adresatów (najczęściej oddzielamy ich przecinkami lub średnikami),
- **Cc** – adresy, do których ewentualnie wysyłana jest kopia listu. Jeżeli program obsługujący pocztę daje taką możliwość – znajduje się dodatkowy składnik, czasami osobny nagłówek, zawierający informację, na jaki adres została wysłana ukryta kopia wiadomości e-mail,
- **Attachments/ Załączniki** – dołączone pliki (załączniki),
- **Subject/ Temat** – temat listu,

Informacje teoretyczne

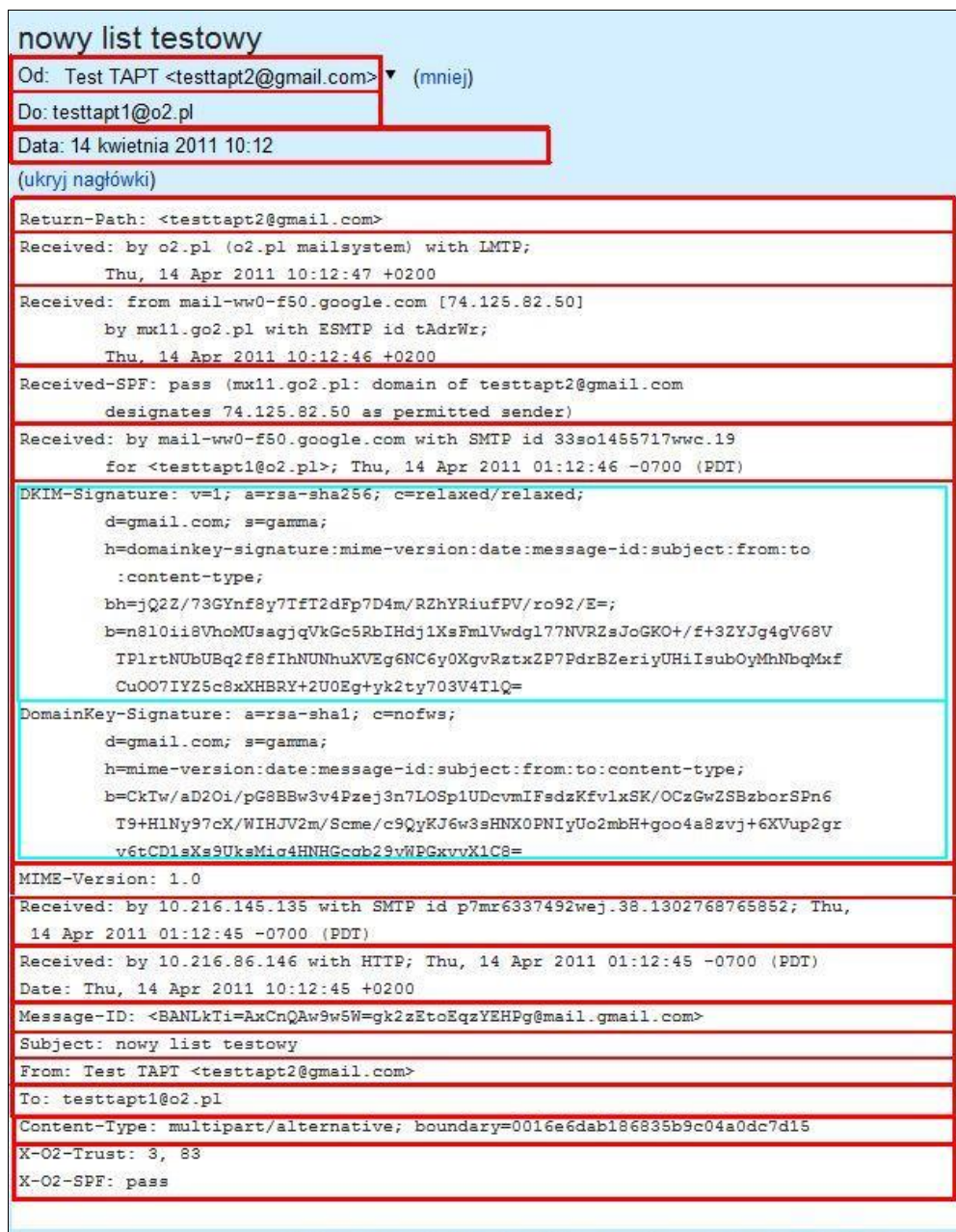
- **Skrzynka poczty elektronicznej** (Mailbox) – obszar pamięci masowej przeznaczony do przechowywania plików zawierających wiadomości internetowe przesyłane za pomocą poczty elektronicznej. Podzielona jest najczęściej na „skrzynki” poczty wychodzącej i poczty przychodzącej. Funkcjonalnie, skrzynka poczty elektronicznej jest odpowiednikiem prawdziwej skrzynki pocztowej.
- **POP3** (Post Office Protocol version 3) – protokół internetowy z warstwy aplikacji pozwalający na odbiór poczty elektronicznej ze zdalnego serwera do lokalnego komputera poprzez połączenie TCP/IP.
- **SMTP** (Simple Mail Transfer Protocol) – tekstowy protokół, w którym określa się, co najmniej jednego odbiorcę wiadomości (w większości przypadków weryfikowane jest jego istnienie), a następnie przekazuje treść wiadomości. Demon SMTP działa najczęściej na porcie 25.
- **Serwer poczty elektronicznej** (Mail Transfer Agent, MTA) – program poczty elektronicznej przesyłający wiadomości internetowe pomiędzy adresami poczty elektronicznej, wykorzystujący architekturę oprogramowania typu klient-serwer. Niepoprawnie skonfigurowany MTA może stanowić tzw. open relay i służyć do rozsyłania spamu.
- **Plik tekstowy** – plik wiadomości.
- **Hop** – skok, wynik działania routerów wyznaczających trasę (Trace) dla pakietów w sposób statyczny (Routing Table Static) lub dynamiczny (Routing Table Dynamic).
- **IP** – adres IP (numer komputera w sieci) w zależności od wersji może 32 bitowy (IP v4) lub 128 bitowy (IP v6).

- **Spam** – niechciana wiadomość najczęściej pochodząca z nieznanego lub zafałszowanego adresu, może zawierać m.in. reklamy, treści pornograficzne, odnośniki do stron internetowych o podejrzanej treści. Spam może być wysłany w celu wyłudzenia informacji przechowywanych w systemie.
- **Remailer** – specjalnie spreparowane serwery służące do zachowania anonimowości przez nadawcę najczęściej wykorzystywane do rozsyłania spamu.

Nagłówki niejawne – części wiadomości, które nie są wyświetlane i zazwyczaj nie budzą zainteresowania przeciętnego użytkownika poczty e-mailowej.

Standardowe pola wiadomości:

- **Return-Path** – (teoretycznie) zawiera adres nadawcy, który jest używany do powiadomienia osoby wysyłającej e-maila w przypadku problemów z jego dostarczeniem. Dla spamu jest on zwykle fałszywy, tak samo jak nagłówek „From”. W przypadku innych wiadomości bywa, że wskazuje na prawdziwego nadawcę, mimo że w nagłówku „From” umieszczono inne dane. Najczęściej pierwsze miejsce fałszerstwa.
- **Delivered-To** – nagłówek wskazuje, na jaką fizyczną skrzynkę na serwerze dostarczono wiadomość. Jest to istotne w przypadku, gdy w nagłówku „To” umieszczono adres będący „Alias” właściwej skrzynki. Analiza tego fragmentu pozwala na weryfikację adres – „Alias”.
- **Received** – każdy serwer, przez który przechodziła wiadomość zwykle zostawia tu informację o sobie (podając swój adres, rodzaj oprogramowania oraz identyfikator wiadomości). Reguła ta nie dotyczy, tzw. „Remailerów”. Może się również zdarzyć, że lista serwerów w nagłówkach „Received” jest celowo zafałszowana, aby trudniej było przeanalizować drogę przesyłki. Część ta wyznacza tor postępowania podczas śledzenia trasy wiadomości. W tym miejscu można odnaleźć adresy IP serwerów, na których weryfikujemy ślady elektroniczne, jakie zostawiła wiadomość po przejściu przez serwery w ich logach systemowych. Najczęściej fałszowane miejsce.
- **Message-ID** – niepowtarzalny identyfikator wiadomości e-mail lub postu na grupie dyskusyjnej. Wykorzystywany najczęściej w przypadku grup dyskusyjnych w celu szybkiego odnalezienia wiadomości. W tym miejscu można odnaleźć identyfikator mogący zweryfikować ślady elektroniczne tj. czy ta konkretna wiadomość przechodziła przez serwer.
- **From, To, Subject** – standardowe nagłówki każdego listu, niemające większego wpływu na poprawne dostarczenie listu. Ich treść, zwłaszcza w przypadku spamu, jest często generowana automatycznie lub jest to losowo wygenerowany ciąg znaków. Części te mogą być wypełniane fikcyjnymi danymi.
- **Content-Type** – zawiera informację o typie przesyłki – jest to wiadomość składająca się z różnego typu danych (czysty tekst i HTML).



Rys. 2. Odkryte wszystkie nagłówki (zaznaczono części) otwarcie przez WWW

- Niebieskie zaznaczenie – sygnatury szyfrowania
- Czerwone zaznaczenie – nagłówki

Nagłówki X

- **X-Original-To** – można z nich odczytać, jaki adres był podany jako adres odbiorcy, zanim lokalny serwer pocztowy przekazał go do skrzynki fizycznej. Będzie to jeden z „Aliasów” pocztowych skojarzonych z fizycznym kontem na serwerze.
- **X-Virus-Scanned** – informacja dotycząca, jaki program antywirusowy i na którym serwerze skanował pocztę pod kątem wirusów.
- **X-Priority** i **X-MSMail-Priority** – informacja, jaki priorytet wiadomości nadał nadawca.
- **X-Mailer** i **X-MimeOLE** – informacja dotycząca programu używanego przez nadawcę (np. Outlook Express). Należy zwrócić uwagę, że oprogramowanie do generowania spamu często podszywa się pod najpopularniejsze programy pocztowe.

Inne

- Należy zauważyć, że daty i godziny w nagłówkach „Received” odpowiadają czasom lokalnym jakie ustawiono na serwerach.
- Sygnatury zawierają jeden i niepowtarzalny identyfikator wiadomości przechowywany na serwerze co pozwala potwierdzić jej obecność nawet jeżeli została usunięta.

Kluczowe elementy nagłówka do analizy

1. **Received:** – lista serwerów, które przetwarzały wiadomość, w kolejności od ostatniego do pierwszego.
2. **Return-Path:** – adres zwrotny używany przez serwer (może różnić się od From:).
3. **Message-ID:** – unikalny identyfikator wiadomości (można sprawdzić jego domenę).
4. **X-Originating-IP:** – oryginalny adres IP nadawcy (często w webmailach).
5. **Date:** – czas wysłania (może ujawniać manipulację).
6. **User-Agent:** – klient poczty lub aplikacja użyta do wysyłki.
7. **Authentication-Results:** – wyniki SPF², DKIM³, DMARC⁴.

Zanim jednak rozpoczniesz szczegółową analizę koniecznym jest utrwalenie – zapisanie dokumentu elektronicznego. List może mieć różne formy wizualne w zależności od formularza i narzędzia w jakim został sporządzony. Przykład listu sporządzonego w formularzu poczty serwisu Onet:



Rys. 3. Brak widoczności elementów stanowiących podstawę analizy

Kolorem niebieskim oznaczono elementy istotne z punktu widzenia analizy. Treść w dolnym prostokącie – zdekodowany link z treści zapisany w formacie html.

-
- ² SPF – (**Sender Policy Framework**) to rekord DNS (typu TXT) w konfiguracji domeny, który autoryzuje serwery pocztowe do wysyłki maili w jej imieniu, zapobiegając podszywaniu się (spoofingowi). Wynik weryfikacji SPF (Pass/Fail) jest widoczny w nagłówkach e-mail, zazwyczaj jako Received-SPF lub w sekcji Authentication-Results.
 - ³ DKIM – Nagłówek **DKIM-Signature** to kryptograficzny podpis dodawany do nagłówków wiadomości e-mail, weryfikujący autentyczność nadawcy oraz integralność treści. Zapewnia, że e-mail nie został zmodyfikowany podczas przesyłania, chroniąc przed phishingiem i spamem. Kluczowe znaczniki to: d= (domena), s= (selektor) i b= (podpis).
 - ⁴ DMARC – Nagłówki DMARC w wiadomościach e-mail (zazwyczaj widoczne jako Authentication-Results) służą do weryfikacji tożsamości nadawcy, sprawdzając spójność domeny w polu "Od" z rekordami SPF i DKIM. Wyniki DMARC (pass/fail) pomagają serwerom odbiorczym wykrywać phishing i podszywanie się pod domenę, a w przypadku niepowodzenia – odrzucić wiadomość (reject) lub przenieść ją do spamu (quarantine).

Co jest istotne i na co zwrócić uwagę po wyświetleniu nagłówka:

- Identyfikator wiadomości.
- Priorytet.
- Znaczniki czasowe wiadomości.
- Ważność wiadomości – kiedy wygasa wiadomość? *Uwaga!! – możemy nie mieć możliwości jej ponownego wyświetlenia.*

```
Return-Path: <gregmatyniak@poczta.onet.pl>
Delivered-To: <marestaw@o2.pl>
X-WP-SR: 60sXR0LnHvzhUUumeBdmfrfAS1608T4DqY55t9RBg0VPkVB16I0MK5mK2Kc=
Received: (wp-smtod mx.tlen.pl 27477 invoked from network): 29 Jun 2025 18:52:30 +0200
Received: from smtpa35.poczta.onet.pl (f213.180.142.351)
  (envelope-sender <gregmatyniak@poczta.onet.pl>)
  by mx.tlen.pl (WP-SMTPD) with ECDHE-RSA-AES256-GCM-SHA384 encrypted SMTP
  for <marestaw@o2.pl>; 29 Jun 2025 18:52:30 +0200
Received: from mta1.m5r2.onet (mta1.m5r2.onet [10.174.35.135])
  by smtp.poczta.onet.pl (Onet) with ESMTP id 4bVb1h5HNBz1hg33
  for <marestaw@o2.pl>; Sun, 29 Jun 2025 18:52:24 +0200 (CEST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=poczta.onet.pl;
  s=2011; t=1751215944;
  bh=P2sUMzjHfdEY56Bm8npZ+ibhi/qAXyqT9wqqUQSyqfw=;
  h=From:To:Subject:Date:From;
  b=p3J1Sp0SZfo2TC0zt1P4WvM10/EfHQHRCncI5z0fBpFv+mo9vGqsHY+uphFpr23e4
  gE8Z8JaUqPISVWq0mpket7juG4mEB5oAnAI0iaYCPGBVJX2OgrQLZPzbDZagrpBYWB
  eyu7LuXZTIyL1ztgHLPTfQLVMcsW1351oxV0qZZI=
X-Mailer: onet.poczta
X-Priority: 3
X-Onet-Pmq: <gregmatyniak@poczta.onet.pl>;46.148.150.161:PI:1
Received: from [46.148.150.161] by mta1.m5r2.onet with HTTP id
  22ee659aa147cf6f; Sun, 29 Jun 2025 18:52:14 +0200
From: Grzegorz Matyniak <gregmatyniak@poczta.onet.pl>
To: marestaw@o2.pl
Subject: Pocztuj mi mamo
Message-ID: <8b590f28-df81-414d-7db5-4151ce88afb5@poczta.onet.pl>
Content-Transfer-Encoding: quoted-printable
Date: Sun, 29 Jun 2025 16:52:24 +0000
MIME-Version: 1.0
Content-Type: text/html; charset=utf-8
X-WP-DKIM-Status: good (id: poczta.onet.pl)
X-WP-MailID: 7df5307f0025ea5c5bfd2ede95dfdc32
X-WP-AV: skaner antywirusowy Pocztuj o2
X-WP-SPAM: NO (A) 1U00010 [oYNk]



Rys. 4. Wyświetlona zawartość listu wraz z nagłówkami



### Jak NIE zabezpieczać wiadomości:

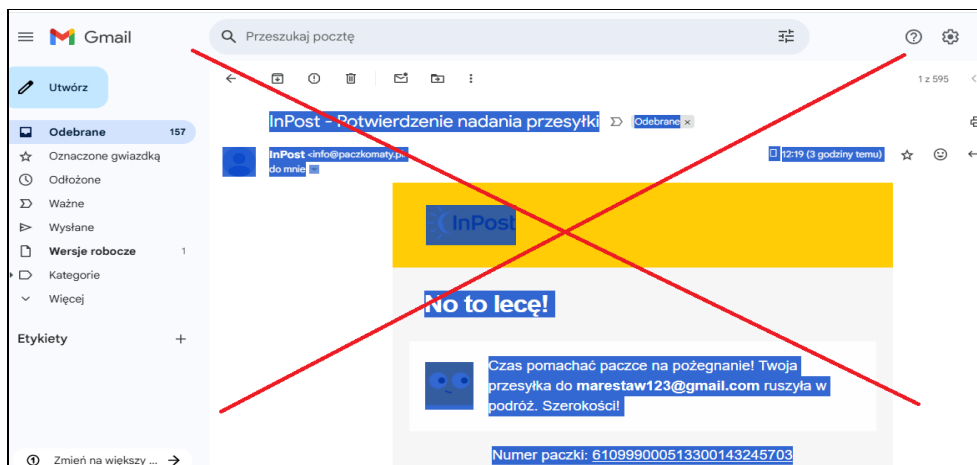


- ✗ Nie robimy zrzutu ekranowego lub fotografii ekranu telefonem!!!
- ✗ Nie wykonujemy zaznaczenia adresu email nadawcy, tematu i tekstu wiadomości – kopiowania i wklejania do innych programów!!!
- ✗ Nie zapisujemy strony z przeglądarki z wyświetloną wiadomością.
- ✗ Nie drukujemy widocznej treści wiadomości.
- ✗ Nie przesyłamy wiadomości nawet na skrzynkę służbową.

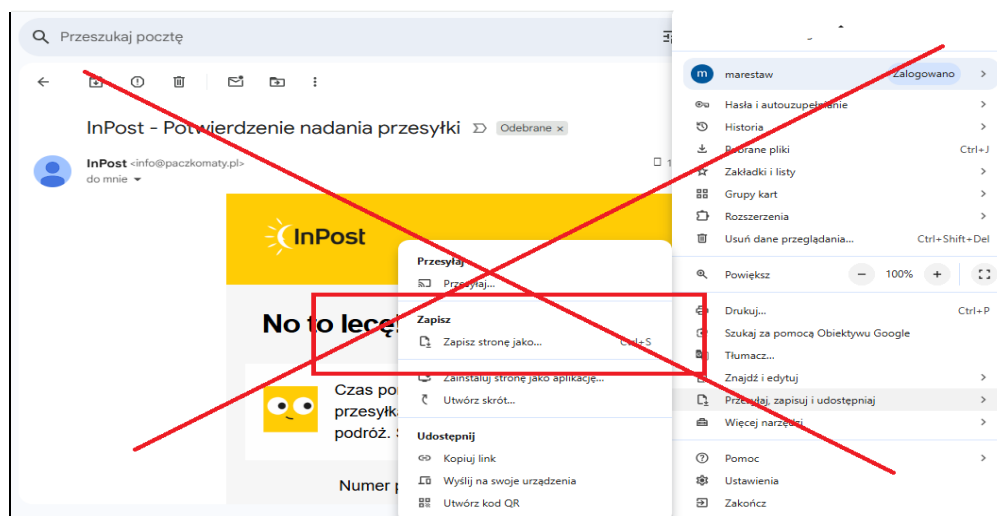


Strona 102


```



Rys. 5. Tak nie zabezpieczymy NAGŁÓWKÓW wiadomości



Rys. 6. Tak również nie zabezpieczymy NAGŁÓWKÓW wiadomości

Zacznijmy od początku – użytkownik poczty dostaje anonimowy list o podejrzaney, zaskakującej treści.

Krok 1 – bez paniki, nie usuwać e-maila, po przeczytaniu należy zapisać list w pełnej wersji wraz z nagłówkami. Powinno się pozostawić podejrzaną wiadomość w skrzynce odbiorczej.

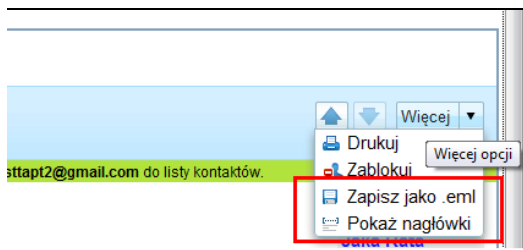
Krok 2 – jeżeli istnieje podejrzenie próby naruszenia prawa, niezwłocznie należy zgłosić incydent informatyczny (może to być przestępstwo lub wykroczenie) odpowiedniemu organowi śledczemu – Policji lub Prokuraturze. Po otrzymaniu takiego zgłoszenia funkcjonariusz jest obowiązany do sporządzenia dokumentacji (może poprosić o otwarcie e-maila w jego obecności lub dostarczenie kopii elektronicznej wiadomości). Co będzie się działo dalej zależy tylko i wyłącznie od wagi zagrożenia, jaką niesie za sobą owa niepożądana informacja e-mailowa.

Krok 3 – tu zaczyna się śledzenie intruza – należy odnaleźć w programie pocztowym opcję pokaż nagłówek lub źródło wiadomości.

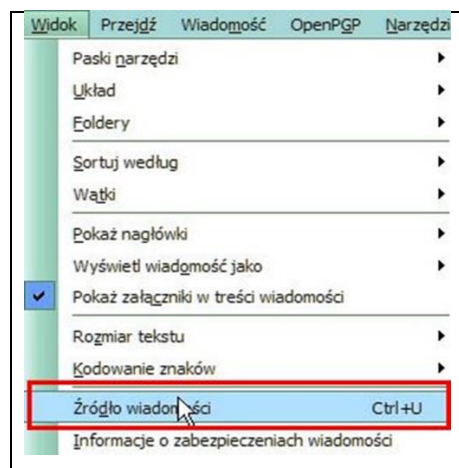
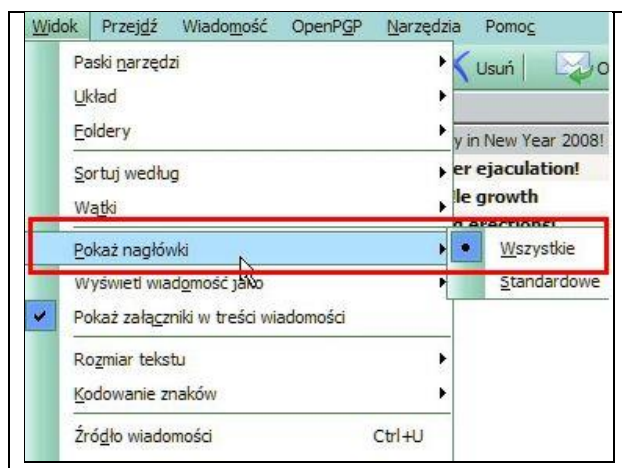
Jak poprawnie zabezpieczyć wiadomość i przygotować ją do analizy?

Sposoby wyświetlenia w programie pocztowym wszystkich nagłówków są definiowane w różnych miejscach programów – klientów poczty, należy jednak szukać możliwości zapisu w formacie eml i opcji wyświetlenia nagłówków. Oczywiście nieodzownym staje się zapisanie wiadomości w formacie domyślnym oferowanym przez oprogramowanie.

Czynności po otwarciu skrzynki i wiadomości aby dotrzeć do nagłówków:

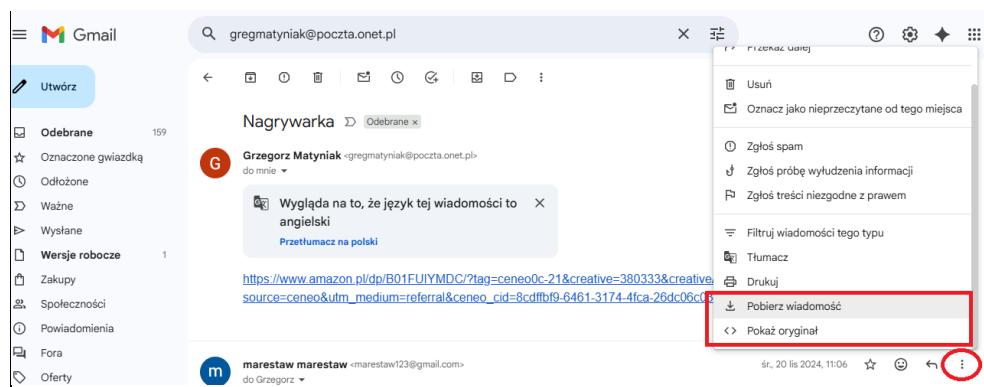


Rys. 7. Zapis oryginalnej wiadomości w formacie eml⁵



Rys. 8, 9. Ustawienie widoku wiadomości w programie kliencie – poczty elektronicznej

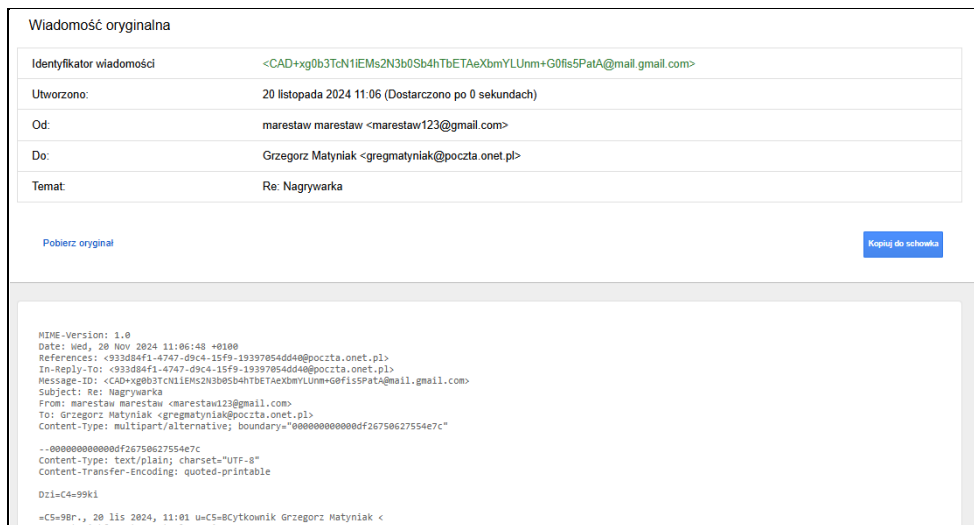
W przypadku otwarcia wiadomości w przeglądarce internetowej wiadomość jest wyświetlana w formie strony www:



Rys. 10. Możliwość pobrania wiadomości i wyświetlenia oryginału

⁵ eml – Plik.eml to standardowy format zapisu pojedynczej wiadomości e-mail, opracowany przez Microsoft, który przechowuje treść, załączniki oraz nagłówki (nadawca, odbiorca, data). Można go otworzyć w programach pocztowych (Outlook, Thunderbird), przez przeciągnięcie do przeglądarki internetowej lub zmieniając rozszerzenie na.mht. Jest powszechnie używany do archiwizacji.

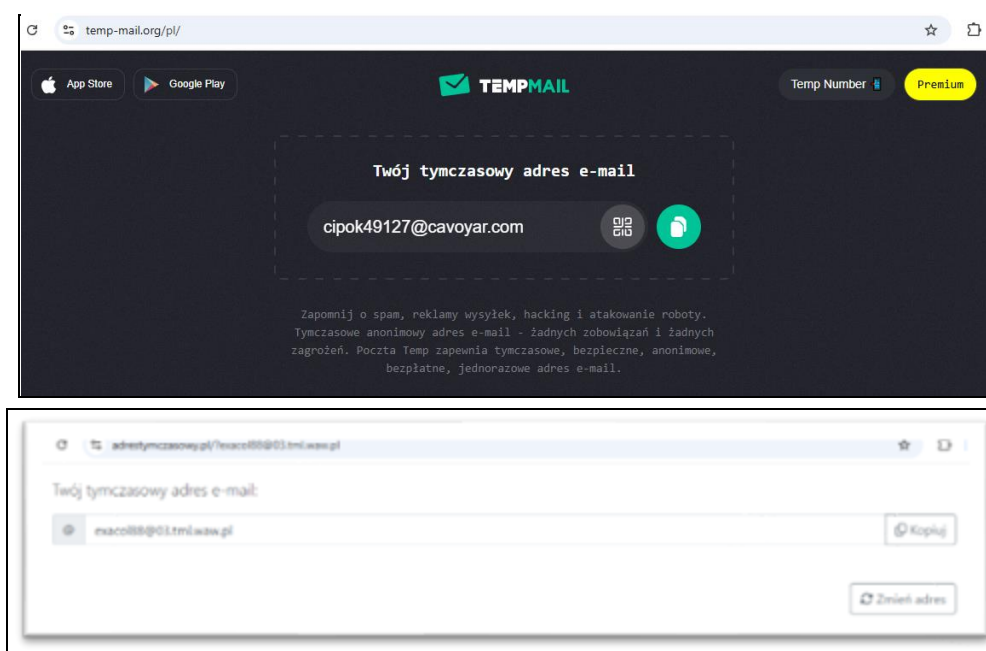
Jeżeli wybierzemy *Pokaż oryginał* to zmieni się sposób wyświetlania wiadomości (fragment widoczny w dolnej części Rys 13) – otrzymamy formę przydatną do analizy – po skopiowaniu tak wyświetlonej zawartości możemy ją wkleić do pliku tekstowego lub bezpośrednio do oprogramowania analitycznego. Widoczna także możliwość pobrania oryginału.



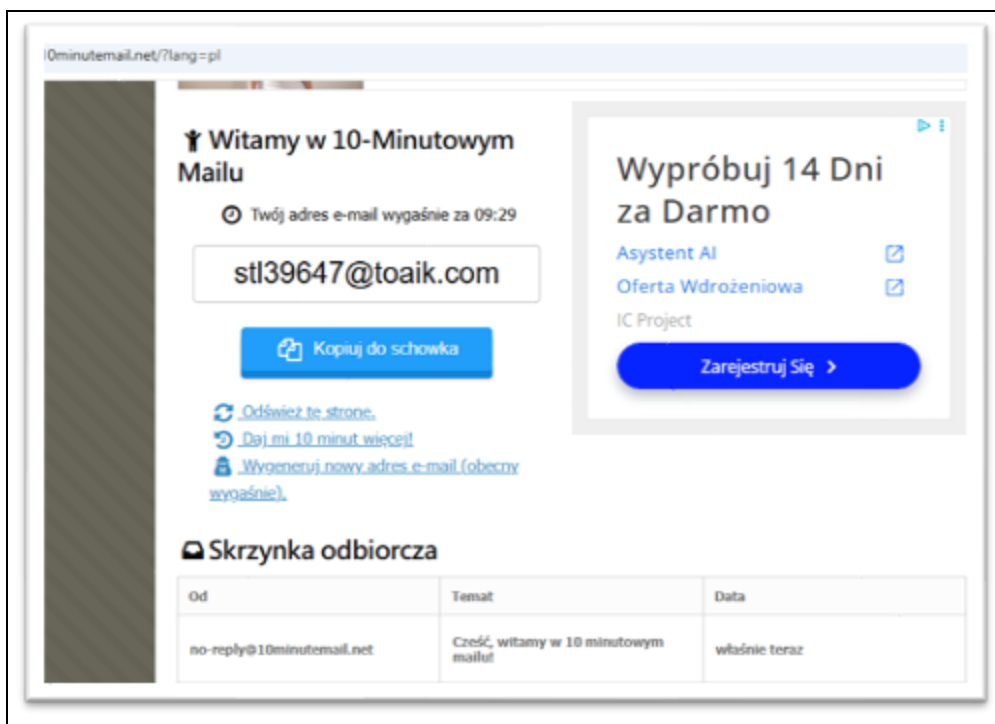
Rys. 11. Oryginał wiadomości w dolnej części format wiadomości gotowy do analizy jeżeli go zapiszesz w pliku tekstowym

Zupełnie osobnym zagadnieniem są wiadomości otrzymywane ze skrzynek „nietrwałych” tak zwanej:

- ✖ poczty 10-minutowej,
- ✖ adresów tymczasowych,
- ✖ wiadomości jednorazowych, które po otwarciu i zapoznaniu się z jej treścią znikają po zamknięciu i nie mamy możliwości ponownie jej otworzyć – (*otwórz-przeczytaj-zamknij-usuń*).



Rys. 12-1, 12-2. Przykłady skrzynek tymczasowych i tzw. 10-minutowych



Rys. 12-3. Przykłady skrzynek tymczasowych i tzw. 10-minutowych

Zawsze warto spróbować zabezpieczyć takie wiadomości nawet jeżeli są one nietrwałe ponieważ mogą wskazać np. serwer proxy⁶, VPN, lub inne cenne dane przydatne w postępowaniu.

Krok 4 – zaznaczenie nagłówka, istotne jest, aby w tym miejscu zaznaczyć cały list (wraz z nagłówkiem) i zapisać go w pliku tekstowym czyli *.txt lub *.eml (w przypadku rozszerzenia eml wiadomość zostanie zapisana w całości wraz z załącznikami).

Krok 5 – uwiarygodnij materiał dowodowy wyliczając sumy kontrolne zabezpieczonych plików i zapisz je na trwałym nośniku (np. na płycie CD lub DVD) wraz sumami kontrolnymi a idealnie byłoby zabezpieczyć jeszcze dokumentację fotograficzną wykonywanych czynności podczas zabezpieczania wiadomości.

Krok 6 – rozpoczęcie analizy trasy e-maila za pomocą nagłówków, które wbrew pozorom są w stanie przekazać wiele istotnych informacji. Jeżeli czynność ta byłaby wykonywana ręcznie, mogłoby to zająć mnóstwo czasu i byłoby oparte na żmudnej, czasochłonnej wykonywanej krok po kroku analizie każdego elementu zawartego w nagłówkach

ANALIZA ŚLEDZCZA WIADOMOŚCI E-MAIL (FORENSIC)

Pozwala podjąć próbę i ustalić:

- skąd faktycznie wyszedł e-mail,
- jaką drogą szedł,
- czy nadawca jest autentyczny,

⁶ Serwer proxy (pośredniczący) to serwer działający jako pośrednik między Twoim urządzeniem a Internetem, odbierający żądania (np. do stron WWW) i przekazujący je dalej w Twoim imieniu, maskując Twój adres IP, co pozwala na omijanie blokad, zwiększenie bezpieczeństwa lub przyspieszenie dostępu przez buforowanie, ale jego bezpieczeństwo zależy od typu (zwykle proxy nie szyfruje danych, w przeciwieństwie do VPN). Działa on na zasadzie "zastępcy", który pobiera zasoby (strony, pliki) i przekazuje je użytkownikowi, często po wcześniejszym zapisaniu ich kopii (buforowanie).

- czy doszło do manipulacji / spoofingu⁷,
- czy to phishing⁸ / BEC⁹ / malware delivery¹⁰,

1. ZABEZPIECZENIE DOWODU (najważniejsze)

- ✗ Nie forwarduj maila.
- ✗ Nie odpowiadaj.
- ✗ Nie klikaj linków.
- ✗ Jeżeli możesz dokumentuj czynności – fotografia.
- ✗ Wylicz sumy kontrolne materiału dowodowego.
- ✗ Zabezpiecz na innym nośniku – np. płyta CD.

Zachowaj:

- pełne **nagłówki (RAW headers)**,
- datę i godzinę odebrania,
- konto odbiorcy,
- klient poczty (Outlook / OWA / Gmail).

2. EKSTRAKCJA NAGŁÓWKÓW

Interesuje nas **CAŁOŚĆ**, w tym:

- Received,
- Message-ID,
- Authentication-Results,
- From / Reply-To / Return-Path,
- DKIM-Signature,
- User-Agent / X-Mailer (jeśli jest,)

Trasa = linie Received (czytaj od DOŁU do GÓRY).

3. REKONSTRUKCJA DROGI WIADOMOŚCI

Dla każdej linii Received sprawdzamy:

- IP nadawcy,
- nazwę hosta,
- strefę czasową,
- opóźnienia między hopami (*skokami*).

⁷ Spoofing to technika cyberprzestępcza polegająca na podszywaniu się pod zaufane osoby, instytucje lub urzędnika (np. bank, policję) w celu wyłudzenia danych logowania, pieniędzy lub zainstalowania złośliwego oprogramowania. Oszuści manipulują danymi identyfikacyjnymi, takimi jak numery telefonów (Caller ID), adresy e-mail czy IP.

⁸ Phishing email – (wiadomość phishingowa) to oszukańcza wiadomość (e-mail, SMS), podszywająca się pod zaufaną instytucję (bank, firmę, agencję rządową), która ma na celu wyłudzenie poufnych danych (hasła, dane karty, dane osobowe) poprzez skłonienie odbiorcy do kliknięcia fałszywego linku, pobrania złośliwego załącznika lub podania informacji na fałszywej stronie imitującej prawdziwą, często tworząc presję czasu i fałszywe poczucie pilności.

⁹ Business Email Compromise – (BEC) to zaawansowane oszustwo cybernetyczne, w którym przestępcy podszywają się pod kadrę zarządzającą, pracowników lub kontrahentów, wykorzystując socjotechnikę do wyłudzenia przelewów lub wrażliwych danych. Ataki są spersonalizowane, za zwyczaj nie zawierają złośliwego oprogramowania, a ich celem jest manipulacja zaufaniem. Skutkują ogromnymi stratami finansowymi i wizerunkowymi dla firm.

¹⁰ E-maile z dostawą złośliwego oprogramowania to złośliwe wiadomości, często przebrane za faktury, powiadomienia o wysyłce lub pilne prośby, zaprojektowane w celu infekowania komputerów ransomware, oprogramowaniem szpiegującym lub trojanami. Za zwyczaj przybywają z za infekowanymi załącznikami (np. Pliki Word, Excel, JAR) lub linkami do złośliwych stron internetowych, które uruchamiają pobieranie, co stanowi 94% wszystkich dostaw złośliwego oprogramowania.

Odpowiadamy na pytania:

- gdzie był **punkt wejścia do SMTP**,
- czy pierwszy serwer to **legalny MTA domeny**,
- czy są **przeskoki geograficzne**.

Pierwszy „Received” = potencjalne źródło (reszta może być spoofowana)

4. WERYFIKACJA TOŻSAMOŚCI NADAWCY

SPF	Czy serwer miał prawo wysyłać w imieniu domeny ? • pass → OK • fail / softfail → spoofing lub relay
DKIM	Czy treść została zmieniona po wysłaniu ? • pass → integralność • fail → manipulacja
DMARC	Czy domena zezwala na taki sposób wysyłki ? • pass → zgodność • fail → naruszenie polityki

5. ANALIZA NAGŁÓWKÓW POMOCNICZYCH

Sprawdzamy:

- Reply-To $\neq$ From → klasyczny phishing,
- dziwny Message-ID (losowe domeny),
- brak User-Agent → automat / skrypt,
- nietypowy X-Originating-IP.

6. KORELACJA CZASOWA

Porównujemy:

- czas wysłania,
- czasy pośrednie,
- czas dostarczenia.

Nienaturalne opóźnienia = relay / proxy / TOR / botnet.

7. WNIOSKI czyli (CO MOŻNA UDOWODNIĆ)

Można UDOWODNIĆ:

- ✓ infrastrukturę wysyłkową,
- ✓ autentyczność domeny,
- ✓ spoofing,
- ✓ phishing / BEC,
- ✓ masową kampanię.

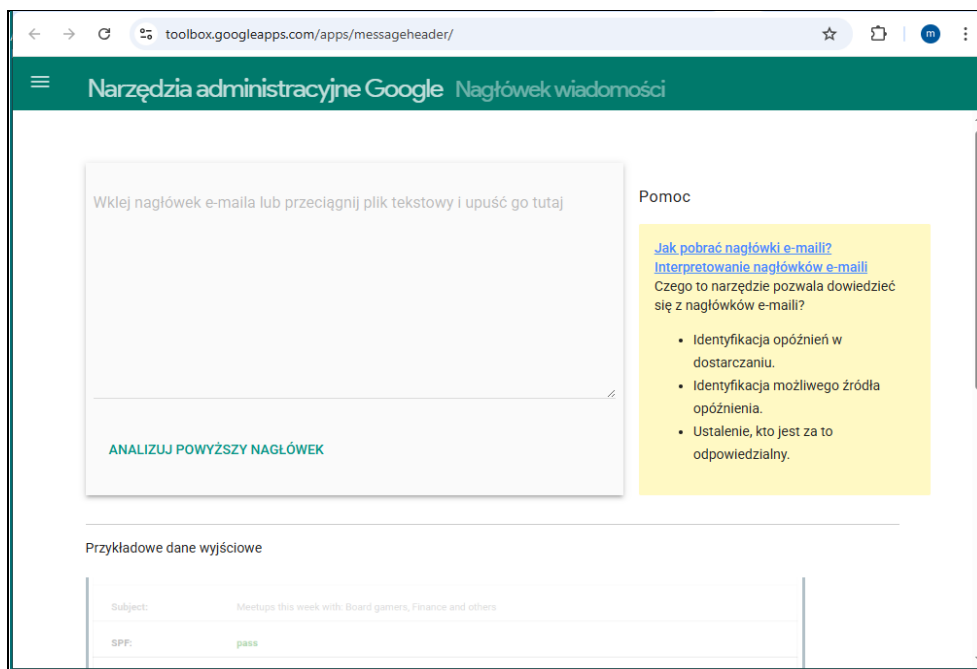
Nie można:

- ✗ wskazać konkretnego komputera użytkownika,
- ✗ obejść TLS,
- ✗ „zobaczyć” treści po drodze.

Poniżej zestawienie **narzędzi do analizy nagłówków** – zarówno online, jak i w formie oprogramowania.

Narzędzia online

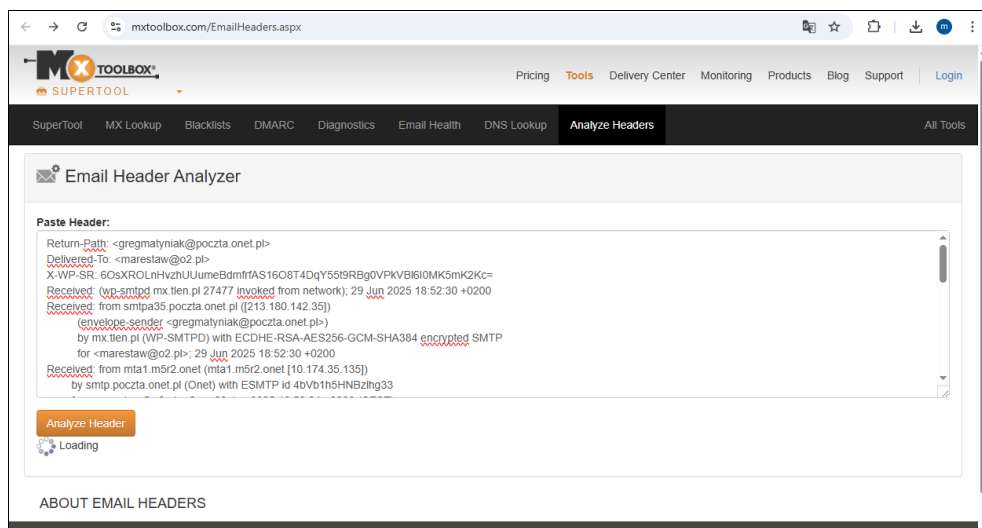
Narzędzie	Funkcje	Plusy	Minusy
Google Admin Toolbox – Messageheader	Wizualizuje trasę e-maila, czasy przeskoku między serwerami, analizuje SPF/DKIM/DMARC.	Darmowe, od Google, prosta obsługa.	Brak zaawansowanej analizy technicznej IP.
MXToolbox – Header Analyzer	Rozbija nagłówek na sekcje, identyfikuje opóźnienia, sprawdza DNS serwerów.	Popularne, dodatkowe testy DNS/SMTP.	Wersja darmowa ograniczona.
Mailheader.org	Minimalistyczny parser nagłówków, pokazuje kolejność serwerów.	Szybki i prosty.	Brak dodatkowych testów reputacji.
G Suite Toolbox Messageheader	Wersja podobna do Google Admin Toolbox, ale przystosowana pod G Suite.	Integracja z Google Workspace.	Skupia się na środowisku Google.
WhatIsMyIP Email Header Analyzer	Analiza IP w Received, identyfikacja hostów.	Łatwa interpretacja IP i lokalizacji.	Brak weryfikacji podpisów DKIM.



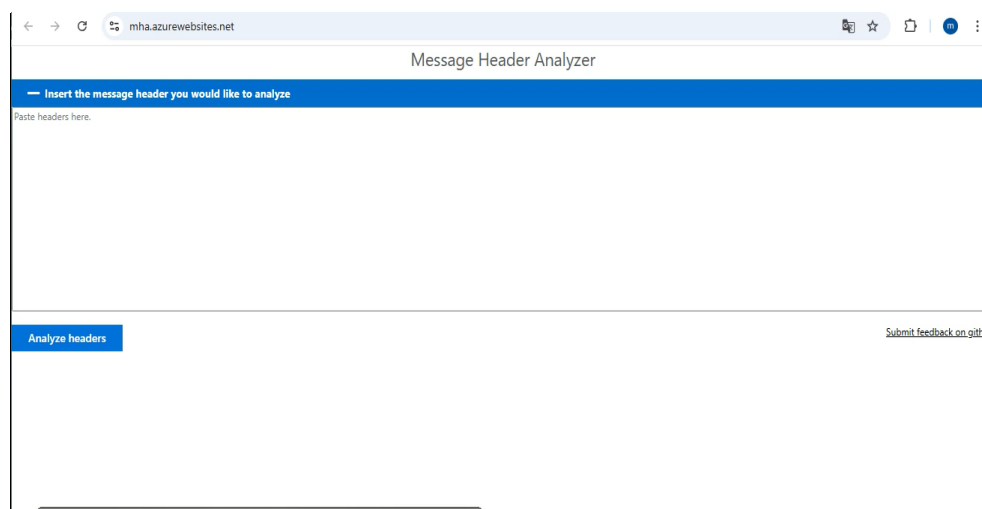
Rys. 13. Ekran roboczy **Google Admin Toolbox – Messageheader**

Przykład pracy z narzędziem

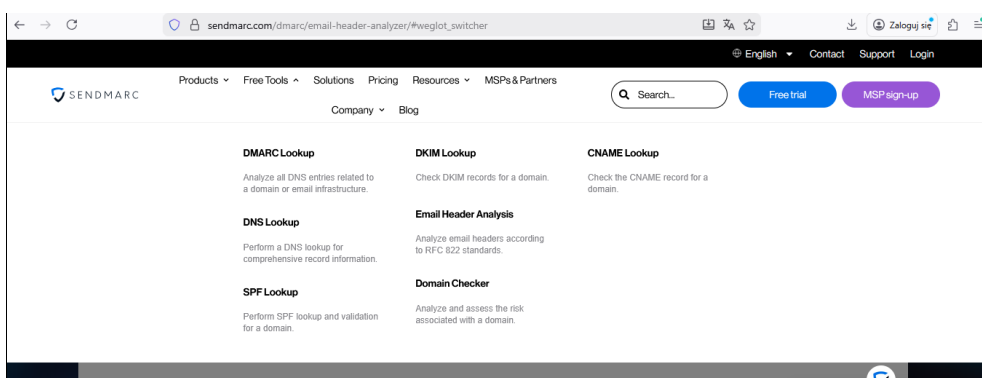
- **Wejście:** Kopiujesz pełny nagłówek z klienta poczty (np. Gmail: *Pokaż oryginał*).
- **Przetwarzanie:** Wklejasz do Google Admin Toolbox lub MXToolbox.
- **Wynik:** Otrzymujesz wizualną trasę, opóźnienia, wyniki SPF/DKIM/DMARC oraz potencjalne adresy IP nadawcy.



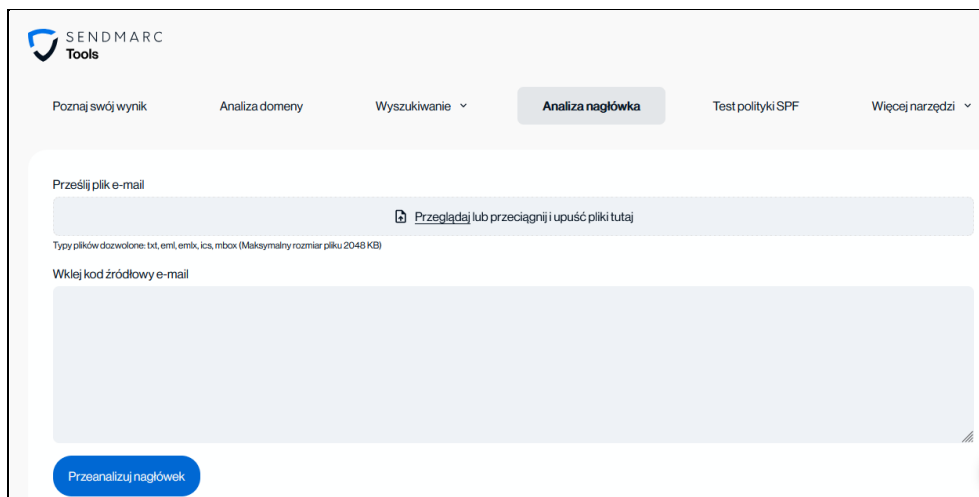
Rys. 14. Ekran roboczy <https://mxtoolbox.com/EmailHeaders.aspx>



Rys. 15. Ekran roboczy MXToolbox – Header Analyzer – <http://mha.azurewebsites.net>



Rys. 16. Ekran Free Tools https://sendmarc.com/dmarc/email-header-analyzer/#weglott_switcher



Rys. 17. Ekran roboczy narzędzia analizy

Oprogramowanie i narzędzia lokalne

Narzędzie	Typ	Funkcje
Exim / Postfix / Sendmail logs	Analiza logów serwera poczty.	Do ręcznej korelacji z nagłówkami.
Wireshark	Sniffer pakietów.	Możliwość podglądu transmisji SMTP.
rfc822-parser (Python)	Biblioteka programistyczna.	Parsowanie nagłówków zgodnie z RFC 822/2822/5322.
Email Header Analyzer (w Hunchly, Maltego, TheHive)	Moduły w większych narzędziach OSINT/DFIR.	Łączy analizę nagłówków z powiązaniami OSINT.
MHA (Mail Header Analyzer)	Skrypt Perl/Python.	Automatyczna analiza Received, SPF, DKIM.

Przykładem kompleksowego narzędzia analitycznego jest **eMailTrackerPro**.



Software, który testowano to 15-dniowa wersja programu **eMailTrackerPro 9.0h** (standard and advanced) działająca pod Windows, koszt licencji wynosi ok. 25\$. Pełna wersja pozwala na całościową weryfikację skrzynki nadawczej i odbiorczej (adresy IP) oraz na kompleksową analizę nagłówka. Producentem programu jest Visualware Inc. Program można pobrać z adresu <http://www.emailtrackerpro.com/>, dostępny jest również *tutorial*. W przypadku skonfigurowania klienta poczty (jak np.: Outlook, The Bat) program integruje się ze skrzynką pocztową i może filtrować spam na podstawie czarnej lub białej listy, stworzonej przez właściciela skrzynki.

Do analizy należy otworzyć zapisaną wcześniej wiadomość. Następnym krokiem jest skopiowanie wcześniej zapisanego w pliku tekstowym nagłówka (Ctrl+C).

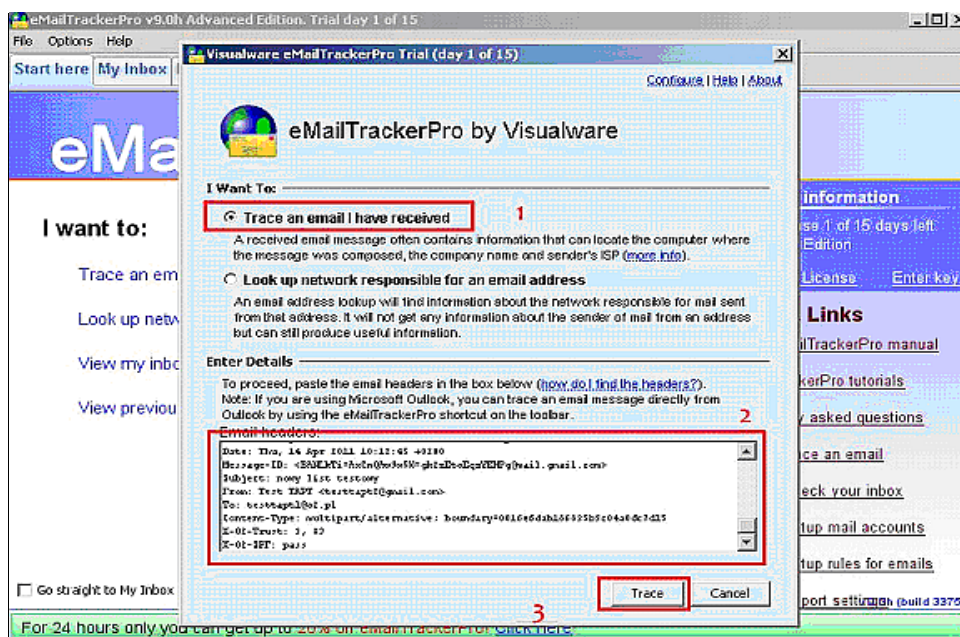
```

Return-Path: <testapt2@gmail.com>
Received: by 92.pl (92.pl mailsystem) with SMTP;
  Thu, 14 Apr 2011 10:12:47 +0200
Received: from mail-wv0-f50.google.com [74.125.82.50]
  by sm11.go2.pl with SMTP id tAdwUw;
  Thu, 14 Apr 2011 10:12:46 +0200
Received-SPF: pass (sm11.go2.pl: domain of testapt2@gmail.com
  designates 74.125.82.50 as permitted sender)
Received: by mail-wv0-f50.google.com with SMTP id 38sol456717wvc.13
  for <testapt2@go2.pl>; Thu, 14 Apr 2011 01:12:46 -0700 (PDT)
MIME-Signature: vml; awwa-sha256; c=relaxed/relaxed;
  d=go2.pl; s=awwa;
  h=domainkey-signature:mime-version:date:message-id:subject:from:to;
  :content-type;
  bh=jQ22/73CYafay7Tf2dFp7D4m/BzhV3iufPV/co92/E=
  b=810i18VhoHJaaagqV6Gc5RbIRd31KsFmVvdgl77NVR2aJoGKO+/432YJgigV66V
  TPlrNDbUBq2f6f1bNUNhuXVEgNG6yGvRctk277PdxS2eriyUHiIaubOymNogMx;
  Cu007Y25c8aXBBRY42U8Eg+yk2ty70Sv4T1Q;
  DomainKey-Signature: awwa-sha1; c=noEva;
  d=go2.pl; s=awwa;
  h=mime-version:date:message-id:subject:from:to:content-type;
  b=CkTv/AD2O/pG8B8w3v4Pae3Sn7LOsp1UDcvaITdaKfVlKX/OCaQwCSBabx8Dd6
  T94H1Ny97cX/NHJV2m/Scme/c9QyK36w3eINDK0PNYUo2mB+qoo4asv+6XUp2g;
  v5cD1aXa8UkaMig4HNRGcqb23yWdGsvvK1C8;
  MIME-Version: 1.0
Received: by 10.216.144.146 with SMTP id w7w633243uej.38.13G2768765852; Thu,
  14 Apr 2011 01:12:45 -0700 (PDT)
Received: by 10.216.144.146 with SMTP id w7w633243uej.38.13G2768765852; Thu,
  14 Apr 2011 01:12:45 -0700 (PDT)
Date: Thu, 14 Apr 2011 10:12:47 +0200
Message-ID: <BAM...>
Subject: nowy list
From: Test TAPC <testapt2@gmail.com>
To: testapt2@go2.pl
Content-Type: multipart/alternative; boundary=00166dab196835b9c04a0dc7d16
X-02-Trust: 3, 80
X-02-SPF: pass

```

Rys. 18. Zaznaczone do kopiowania i analizy nagłówki listu

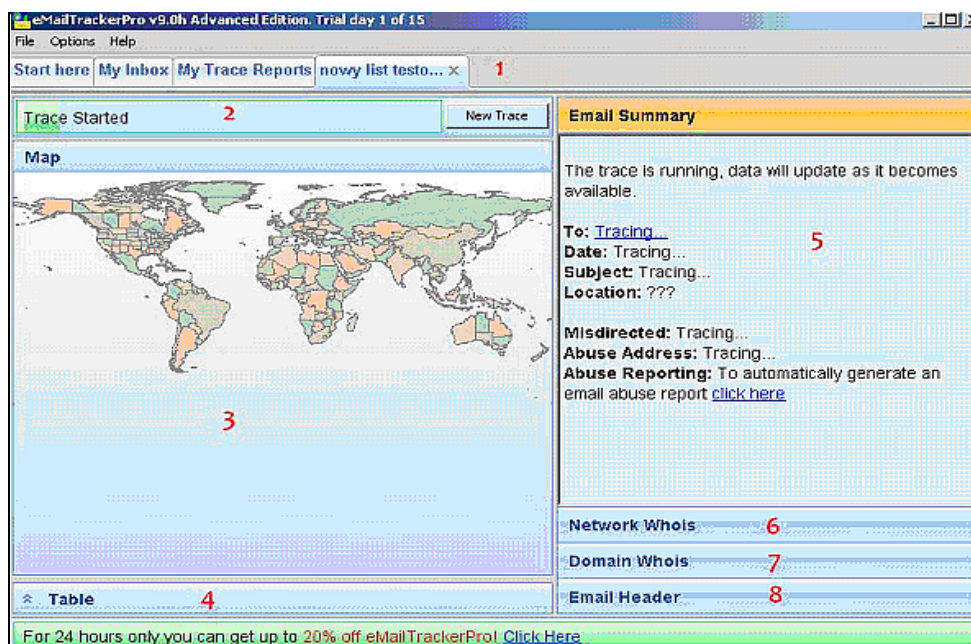
Po pojawieniu się okna programu wybrać 1 i w miejscu 2 wkleić (Ctrl+V) element wcześniej skopiowany. Po wykonaniu powyższych czynności należy wybrać 3 (Trace).



Rys. 19. Pierwszy ekran, do którego należy wkleić skopiowaną zawartość

1. Trasa e-maila na podstawie nagłówków.
2. Wprowadzenie „detali” – okno, do którego wklejamy skopiowany nagłówek.
3. Trasa.

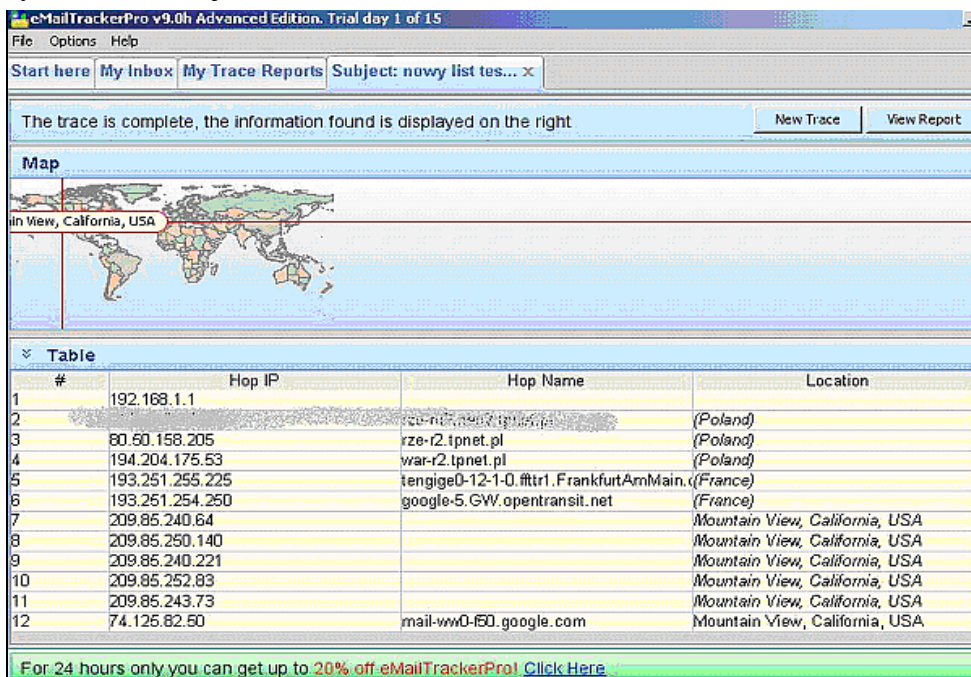
Nastąpi zmiana okna programu, rozpoczyna się analiza:



Rys. 20. Analiza trasy na podstawie informacji zawartych w nagłówkach

1. Menu zakładek.
2. Pasek postępu i informacji.
3. Okno mapki z geolokalizacją.
4. Zakładka gdzie pojawi się lista adresów IP o raz nazw hostów.
5. Sumaryczna informacja o emailu.
6. Do kogo należy sieć.
7. Do kogo należy domena.
8. Nagłówek listu.

Każde przejście od nadawcy do adresata do nagłówek listu dodaje segment oznaczony „Recevide” (wraz z data, godziną oraz adresem IP komputera). Po zakończeniu analizy zostaje wyświetlona lista „Hopów” – (skoków), przez które przeszedł niepożądany list zanim znalazł się w skrzynce odbiorczej.



Rys. 21. Część okna programu z mapką i tabelą po analizie

- Pozycje początkowe listy Hop'ów to adresy IP komputera który dokonał analizy, końcowy to adres IP nadawcy listu.

Na mapie, która zostaje wygenerowana podczas działania programu pojawia się geolokalizacja wskazująca miejsce serwera, z którego została wysłana wiadomość.

Narzędzie w obsłudze jest intuicyjne i mocną jego stroną pozostaje wskazana powyżej geolokalizacja i automatyka generowanych raportów.

Uproszczona lista kroków analityka korzystającego – **emailTrackerPro**:

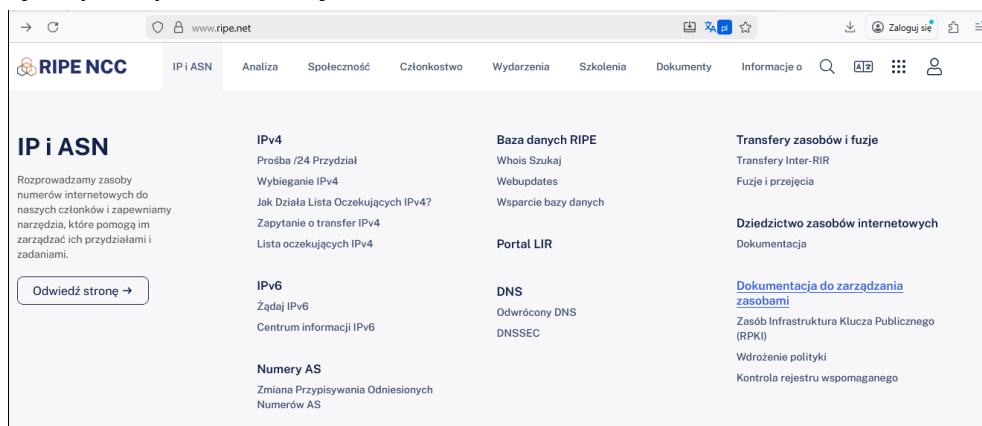
- ✓ Wklej nagłówki do programu.
- ✓ Wybierz trasowanie.
- ✓ Wygeneruj raport.
- ✓ W raporcie rozwiń wszystkie części.
- ✓ Przeglądaj raport w przeglądarce.
- ✓ Wydrukuj raport na drukarce.
- ✓ Zapisz raport jako dokument pdf.

Jeśli po analizie nagłówka listu elektronicznego chcemy przyjrzeć się bliżej jakiemuś adresowi IP, możemy wspomóc się usługą **whois**¹¹.

Świat został podzielony pomiędzy trzy organizacje (stanowiące instytucję RIPE) zajmujące się administracją adresami IP:

- Europa i Afryka to <http://www.ripe.net>;
- Ameryka to <http://www.arin.net>;
- Azja i Pacyfik to <http://www.apnic.net>.

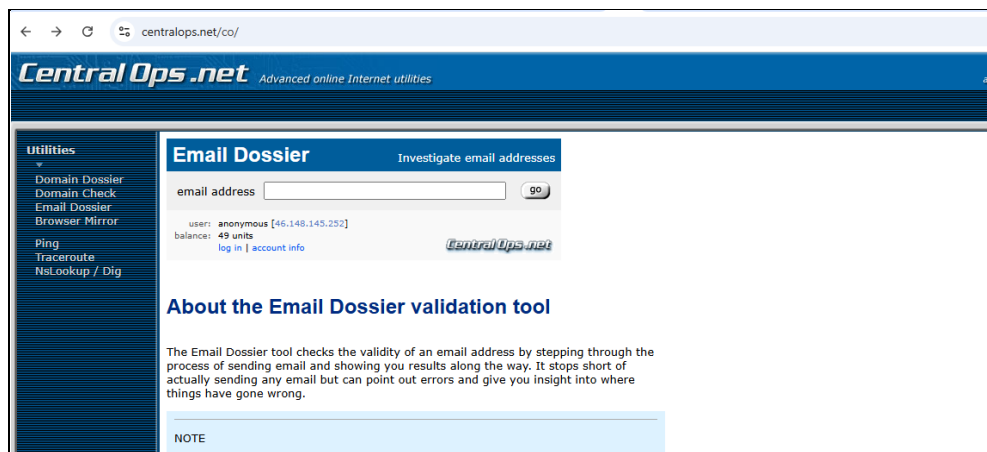
Po wpisaniu do formularza na stronie instytucji RIPE adresu otrzymamy możliwość weryfikacji uzyskanych informacji.



Rys. 22. Wygląd strony <http://www.ripe.net>

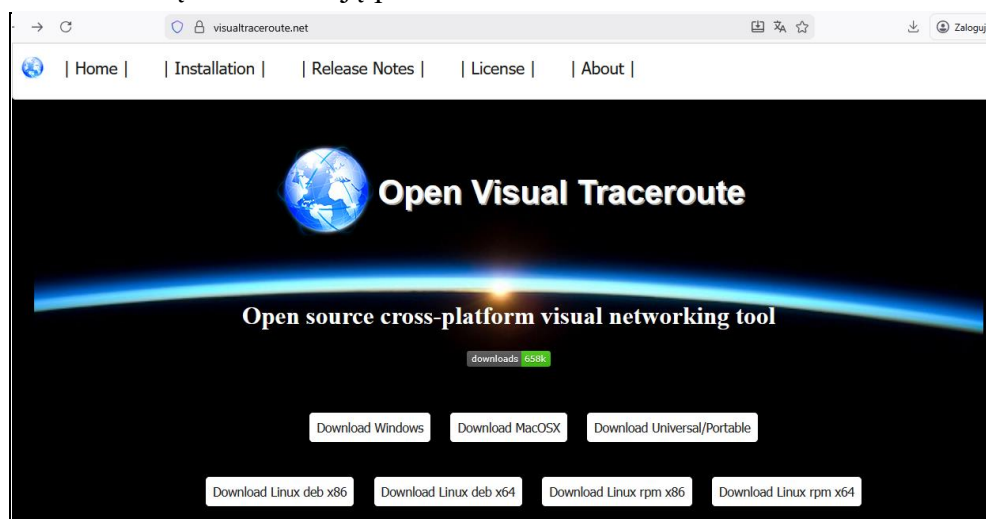
Czynności sprawdzające możemy także wykonać na stronie <http://centralops.net> gdzie zakres możliwości sprawdzania jest dość szeroki między innymi: domena, trasa, itd. widoczne po lewej stronie.

¹¹ WHOIS to standardowy protokół internetowy używany do odpytywania baz danych, które przechowują informacje o zarejestrowanych użytkownikach zasobów internetowych, przede wszystkim adresach IP i nazwach domen.



Rys. 23. Wygląd strony <http://centralops.net>

Wizualizację geolokalizacji adresów znalezionych w nagłówkach listu elektronicznego możemy uzyskać korzystając z oprogramowania **Open Visual Traceroute**. Oprogramowanie jest dostępne na zasadach GPL-GNU pod adresem <https://visualtraceroute.net> jako narzędzie wieloplatformowe włącznie z wersją portable.



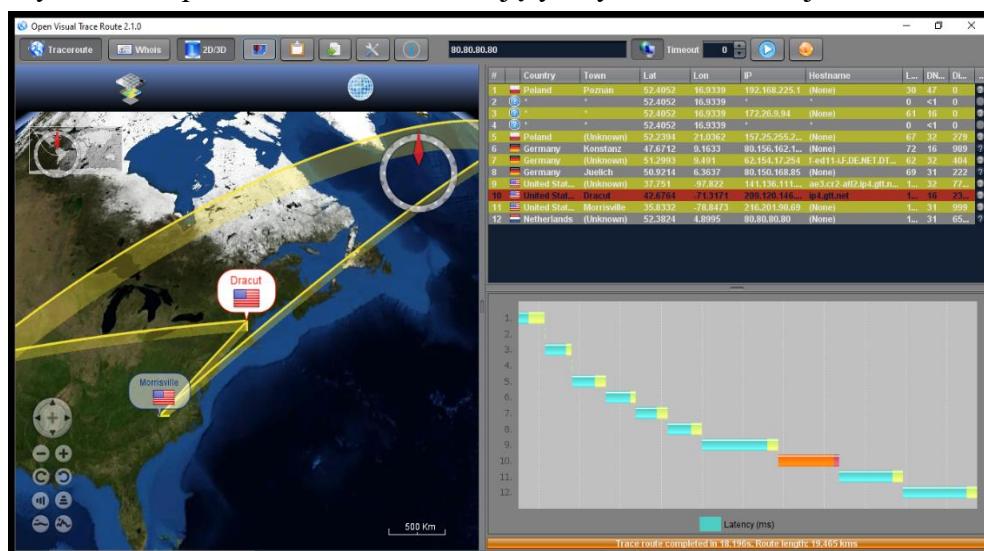
Rys. 24. Strona startowa serwisu z wyborem instalatorów

Open Visual Traceroute to graficzne narzędzie diagnostyczne używane do śledzenia trasy pakietów sieciowych od komputera użytkownika do serwera docelowego. W przeciwieństwie do tekstowego *tracert*, wizualizuje ono trasę na mapie 3D, pokazując poszczególne routery (*przeskoki*) oraz czas ich odpowiedzi. Pomaga zdiagnozować opóźnienia i awarie sieciowe. Kluczowe funkcje Open Visual Traceroute:

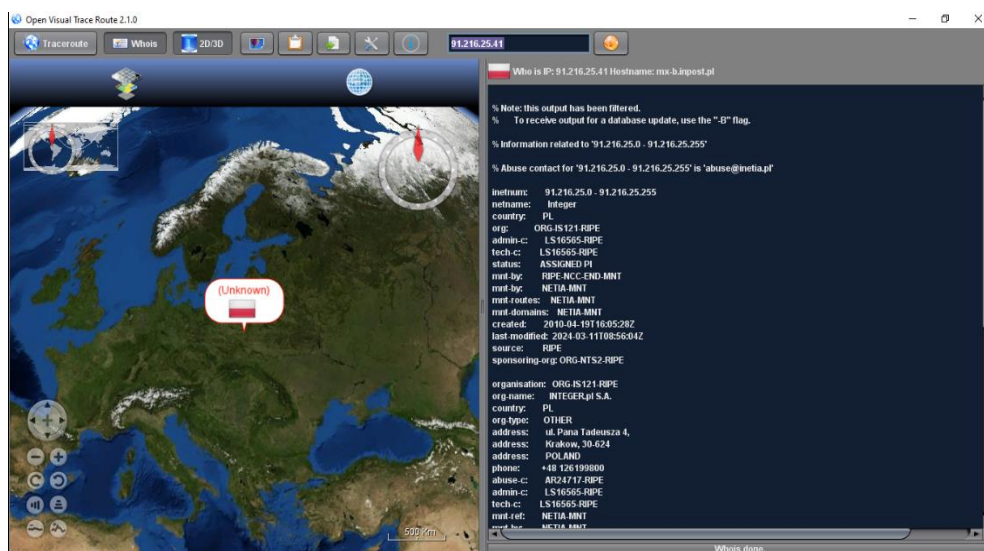
- **Wizualizacja 3D:** Przedstawia drogę pakietów w formie graficznej, ułatwiając lokalizację geograficzną węzłów sieciowych.
- **Diagnostyka połączeń:** Umożliwia sprawdzenie, czy sygnał poprawnie dociera do celu i gdzie następuje zerwanie komunikacji (np. dostawca Internetu, serwer docelowy).
- **Analiza czasu:** Pokazuje opóźnienia (latency) na poszczególnych etapach, co pozwala zidentyfikować „wąskie gardła”.
- **Funkcjonalność:** Działa na zasadzie wysyłania pakietów z rosnącym czasem życia (TTL), badając odpowiedzi od routerów pośrednich.

Narzędzie jest szczególnie przydatne dla administratorów sieci i użytkowników chcących zlokalizować przyczynę problemów z dostępem do stron lub serwerów. W pracy analitycznej pozwala na weryfikację i zobrazowanie położenia (przybliżonego) adresu IP urządzenia, którego adres badamy. Możemy także prześledzić potencjalną drogę – trasę wiadomości, itd. ilustrując ją na mapie 3D.

Ciekawą funkcją jest wbudowane narzędzie sprawdzenia *whois*. Oprogramowanie pozwala wykonać i zapisać zrzut ekranu ilustrujący uzyskane informacje.



Rys. 25. Ekran roboczy – widoczna wytyczona trasa do wskazanego adresu IP wraz z tabelą skoków i opóźnień



Rys. 26. Ekran roboczy wskazujący geolokalizację i informacje z *whois* dla wskazanego adresu IP

Jak czytać całe nagłówki poczty e-mail – przykład analizy „ręcznej”

W nagłówku e-maila jest określony adresat wiadomości, a także rejestrowana jest ścieżka, którą wiadomość podąża podczas przekazywania jej z serwera na serwer. Aby prześledzić tę ścieżkę w kolejności chronologicznej, zacznij czytać od dołu nagłówka i kieruj się ku górze.

Oto przykładowy nagłówek e-maila, którego nadawcą jest KOWALSKI@emailprovider.com, a odbiorcą NOWAK@gmail.com:

Delivered-To: NOWAK@gmail.com

Received: by 11.38.88.31 with SMTP id e3cs239nzb; Tue, 29 Mar 2010 14:11:47 -0800 (PST)

Return-Path:

Received: from mail.poczta Providerr.com (mail.poczta Providerr.com [123.123.123.123]) by mx.gmail.com with SMTP id h19si826631rnb.2010.03.29.14.11.46; Tue, 29 Mar 2010 14:11:47 -0800 (PST)

Message-ID: <20100329231145.26806.mail@mail.poczta Providerr.com>

Received: from [22.22.222.222] by mail.poczta Providerr.com via HTTP; Tue, 29 Mar 2010 14:11:45 PST

Date: Tue, 29 Mar 2010 14:11:45 -0800 (PST)

From: Pan KOWALSKI

Subject: Wiadomość testowa

To: Pan NOWAK

W powyższym przykładzie nagłówki zostały umieszczone w wiadomości trzy razy:

Gdy pan KOWALSKI napisał e-maila

Date: Tue, 29 Mar 2010 14:11:45 -0800 (PST)

From: Pan KOWALSKI

Subject: Wiadomość testowa

To: NOWAK

Gdy e-mail był przesyłany przez serwery dostawcy usług pocztowych pana KOWALSKIEGO (mail.poczta Providerr.com)

Message-ID: <20100329231145.26806.mail@mail.poczta Providerr.com>

Received: from [22.22.222.222] by mail.poczta Providerr.com via HTTP; Tue, 29 Mar 2010 14:11:45 PST

Gdy wiadomość została przesłana od dostawcy usług pocztowych pana KOWALSKIEGO na konto Gmaila pana NOWAKA

Delivered-To: NOWAK@gmail.com

Received: by 11.38.88.31 with SMTP id e3cs239nzb; Tue, 29 Mar 2010 14:11:47 -0800 (PST)

Return-Path: KOWALSKI@poczta Providerr.com

Received: from mail.poczta Providerr.com (mail.poczta Providerr.com [123.123.123.123]) by mx.gmail.com with SMTP id h19si826631rnb; Tue, 29 Mar 2010 14:11:47 -0800 (PST)

Poniżej znajduje się opis poszczególnych sekcji nagłówka wiadomości:

Delivered-To: NOWAK@gmail.com

Adres e-mailowy, pod który wiadomość zostanie dostarczona.

Received: by 11.38.88.31 with SMTP id e3cs239nzb;

Tue, 29 Mar 2010 14:11:47 -0800 (PST)

Czas dotarcia wiadomości do serwerów Gmaila.

Return-Path:

[Adres nadawcy wiadomości.](#)

Received: from mail.poczta Providerr.com

(mail.poczta Providerr.com [123.123.123.123])

by mx.gmail.com with SMTP id h19si826631rnb.2010.03.29.14.11.46;

Tue, 29 Mar 2010 14:11:47 -0800 (PST)

Serwer Gmaila otrzymał wiadomość z serwera mail.poczta Providerr.com 29 marca roku 2010 około godziny 14:00.

Message-ID: 20100329231145.26806.mail@mail.poczta Providerr.com

Unikatowy numer identyfikacyjny przypisany wiadomości przez serwer mail.poczta Providerr.com.

Received: from [22.22.222.222] by mail.poczta Providerr.com via HTTP;

Tue, 29 Mar 2010 14:11:45 PST

Pan KOWALSKI napisał wiadomość za pomocą programu do redagowania e-maili. Następnie serwery mail.poczta Providerr.com otrzymały wiadomość.

Date: Tue, 29 Mar 2010 14:11:45 -0800 (PST)

From: Pan KOWALSKI

Subject: Wiadomość testowa

To: Pan NOWAK

Data, nadawca, temat i adresat – pan KOWALSKI wprowadził te informacje (poza datą) podczas tworzenia wiadomości.

Przykłady wiadomości

Przykład 1. Podszycie – podanie się za kogoś innego

Od: Piotr Kowalski <prof.piotr.kowalski@wp.pl>

Do: diks44 <diks44@wp.pl>

Data: Środa, 11 Marca 2009 14:11

Return-Path: <prof.piotr.kowalski@wp.pl>

Date: Wed, 11 Mar 2009 14:11:41 +0100

Message-ID: <49b7b88d70bdf9.80056452@wp.pl>

MIME-Version: 1.0

Content-Type: text/plain; charset=iso-8859-2

Content-Transfer-Encoding: 8bit

Content-Disposition: inline

X-Mailer: Interfejs WWW nowej poczty Wirtualnej Polski

X-User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; pl; rv:1.9.0.7) Gecko/2009021910 Firefox/3.0.7

Organization: Nowa Poczta Wirtualnej Polski S.A. <http://www.wp.pl/>

X-WP-IP: 89.79.54.55

X-WP-AV: skaner antywirusowy poczty Wirtualnej Polski S. A.

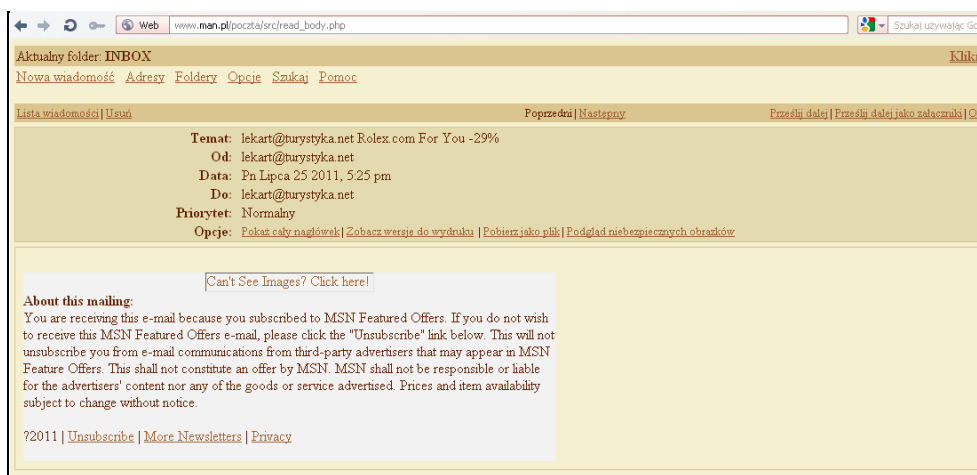
Temat: (brak tematu)

Sprawa studentów jednej z uczelni wyższych

Po sprawdzeniu okazuje się, że rzekomy autor listu ma inny login i nigdy takiego listu nie wysyłał. Pozostaje ustalić z adminem WP z jakiego IP przyszło – potwierdzić ustalenia. Jeżeli lista nagłówek jest krótka można sądzić, że jest to w obrębie tego samego serwera. Należy także podejrzewać, że jest to osoba z otoczenia adresata, znająca jej sekret, upodobania i przyzwyczajenia, etc.

Przykład 2. „List do siebie” – nagłówek z przekierowaniem wewnętrznym

Return-Path: <lekart@turystyka.net>
X-Original-To: lekart@turystyka.net
Delivered-To: lekart@turystyka.net
Received: from poczta.man.pl (debian [62.168.41.37])
by poczta.man.pl (Postfix) with ESMTP id 2DF7A2A2DBB1
for <lekart@turystyka.net>; Mon, 25 Jul 2011 17:25:03 +0200 (CEST)
X-Greylist: delayed 302 seconds by postgrey-1.24 at man; Mon, 25 Jul 2011 17:25:02 CEST
Received: from host17-167-static.23-87-b.business.telecomitalia.it (host17-167-static.23-87-b.business.telecomitalia.it [87.23.167.17])
by poczta.man.pl (Postfix) with ESMTP id 734AF2A2DBA4
for <lekart@turystyka.net>; Mon, 25 Jul 2011 17:25:02 +0200 (CEST)
From: lekart@turystyka.net
To: lekart@turystyka.net
Subject: lekart@turystyka.net Rolex.com For You -29%
Mime-Version: 1.0
Content-type: text/html; charset="utf-8"
Content-Transfer-Encoding: 7bit
X-Antivirus: avast! (VPS 110725-0, 25/07/2011), Outbound message
X-Antivirus-Status: Clean
Message-Id: <20110725152502.734AF2A2DBA4@poczta.man.pl>
Date: Mon, 25 Jul 2011 17:25:02 +0200 (CEST)
X-Virus-Scanned: ClamAV using ClamSMTP



Rys. 27. List¹², którego nagłówek analizowano powyżej

Podsumowując: metodyka postępowania w celu ustalenia miejsca wysłania e-maila z wykorzystaniem programu wspomagającego analizę nagłówek

Do jednostki organizacyjnej Policji zgłosił się poszkodowany który na swoją skrzynkę pocztową otrzymał e-maile z treściami zawierającymi groźby karalne pod jego adresem.

Od pokrzywdzonego przyjąć protokół zawiadomienia o przestępstwie, w zawartości którego powinny znaleźć się następujące treści:

- Jaka jest treść otrzymanego listu na skrzynkę zgłaszającego.
- Jakie jest adres IP komputera zgłaszającego i kto jest dostawcą Internetu dla zgłaszającego.
- Na jakiej stronie internetowej (lub w jakiej usłudze) osoba zgłaszająca posiada skrzynkę pocztową.
- Jaki jest jego adres poczty elektronicznej (e-mail).

¹² Źródło własne

- Czy znana jest jej osoba od której otrzymała wiadomość e-mailową będącą przedmiotem zgłoszenia – czy takich wiadomości było w przeszłości więcej – jeżeli tak to czy nadal je posiada.
- Czy zgłaszający kontaktował się z nadawcą listu (oczywiście jeżeli zna tę osobę lub posiada przypuszczenia co do sprawcy – nadawcy listu z groźbami – jeżeli tak to w jaki sposób;
 - a. w przypadku korespondencji drogą elektroniczną (e-mail) dokonać zabezpieczenia wszelkiej korespondencji posiadanej przez przesłuchiwanego (poprzez dokonanie wydruków i ich dołączenie do zebranych materiałów – możliwe jest ich późniejsze dostarczenie przez pokrzywdzonego);
 - b. telefonicznie – ustalić numer telefonu z którego korzystał pokrzywdzony jak też numer telefonu jakim posługiwał się sprawca lub jaki wskazywał do kontaktów;
 - c. jeżeli były wymieniane SMS-y dokonać ich zabezpieczenia poprzez np.:
 - sfotografowanie całości wraz z numerem telefonu z którego je przesłano,
 - w przypadku korespondencji prowadzonej z wykorzystaniem komunikatorów internetowych np. **WhatsApp, Signal, Messenger** itd. jakim loginem, nickiem posługiwał się pokrzywdzony a jakim sprawca, jeżeli zgłaszający posiada korespondencję to dążyć do jej wydruku i dołączenia do materiałów. Korespondencja ta może potwierdzić lub wskazać inne skrzynki poczty elektronicznej używane przez potencjalnego sprawcę;
- Czy po otrzymaniu wiadomości kontaktował się z nadawcą listu (listów) – w jaki sposób i kiedy, jeżeli była to korespondencja e-mailowa w miarę możliwości dokonać jej zabezpieczenia poprzez wydruki, które mogą stanowić załącznik do protokołu.

Od zgłaszającego należy uzyskać następującą dokumentację związaną ze zdarzeniem:

- Wszelkie wydruki związane z otrzymanymi wiadomościami (w formie wydruków komputerowych).
- Wszelkie wydruki wiadomości od sprawcy otrzymane od sprawcy, gdyż zazwyczaj będzie się tam znajdował adres IP osoby wysyłającej wiadomość.

Możliwa jest sytuacja kiedy zgłaszający nie będzie posiadał przy sobie wszystkich wskazanych dokumentów i w tym przypadku należy zobowiązać go do jak najszybszego dostarczenia przedmiotowych dokumentów w ramach czynności sprawdzających (art. 307 k.p.k).

- Wskazane jest uzyskanie szczegółowego nagłówka otrzymanej (lub otrzymanych) wiadomości od sprawcy w formie elektronicznej (co jest bardzo ważne) – jeżeli chcemy skorzystać z opisanego wyżej programu analitycznego – pozyskanie wersji elektronicznej wiadomości może i powinno nastąpić poprzez otwarcie skrzynki pocztowej przez pokrzywdzonego zawierającej list (listy) od sprawcy oraz sporządzenie ich wersji w formie elektronicznej (np. poprzez zapisanie w programie np.: Notatnik lub *.eml) a następnie nagranie tegoż dokumentu na nośnik (np.: płyta CD-R) lub też zobowiązanie zgłaszającego do dostarczenia wiadomości w takiej formie.

Mając tak zabezpieczoną treść wiadomości – wykorzystując opisany program analityczny dokonać analizy nagłówków i sporządzić wydruk raportu, który należy dołączyć do materiałów dotyczących sprawy wraz z notatką z analizy i ustaleń co do adresów IP (za pomocą np.: strony <http://www.ripe.net> lub <http://www.centralops.net>).

Na podstawie wykonanych czynności i uzyskanych wyników z analiz i sprawdzeń po wszczęciu postępowania wystąpić poprzez prokuraturę o zabezpieczenie i nadesłanie danych od providerów świadczących usługi w tym zakresie, a przede wszystkim osoby, która mogła wysłać list z groźbami.

Pamiętaj! Liczy się czas a obowiązujące prawo to:

Dz.U.2024.1221 USTAWA z dnia 12 lipca 2024 r. Prawo komunikacji elektronicznej

Bibliografia

Literatura:

- Boniewicz A. Analiza śledcza urządzeń mobilnych, Wydawnictwo Helion, Gliwice 2023.
- Comer D. E. Sieci komputerowe TCP/IP – zasady, protokoły, architektura – WNT, Warszawa 1997.
- Craig H. TCP/IP Administracja sieci- Oficyna wydawnicza READ ME – Łódź 1998.
- DiMaggio J. Sztuka wojny cyfrowej, Wydawnictwo Helion – Gliwice 2023.
- Johansen G. Informatyka śledcza, Wydawnictwo Helion, Gliwice 2024.
- Kosiński J. Paradygmaty cyberprzestępczości, Warszawa 2015.
- Meredith D. OSINT w praktyce. Wydawnictwo Helion – Gliwice 2025.
- Oettinger W. Informatyka śledcza, Wyd. II, Wydawnictwo Helion, Gliwice 2024.
- Parker T. TCP/IP – Wydawnictwo Helion – Gliwice 1997.
- Rupik P. Listy w pajęczynie. CHIP, 3/2005.
- Sheldon T. Wielka encyklopedia sieci komputerowych – Wydawnictwo Robomatic – Łódź 1995.
- Stevens W. R. Biblia TCP/IP, t. I, WNT, Warszawa 1997.
- Troia V. Upoluj cyberprzestępcę, Wydawnictwo Helion – Gliwice 2022.
- Wosiński K. Bezpieczeństwo osób i systemów IT z wykorzystaniem białego wywiadu PWN Warszawa 2024.
- Wójcik D. Analiza kryminalna w praktyce: Problemy kryminalistyki 2022.

Źródła internetowe:

- <http://www.emailtrackerpro.com/video/demotest/demotest.swf>
- http://kik.pcz.czest.pl/Slawomir_Litwinski/4-ping-traceroute.pdf
- <http://nie-spamuj.eu/pdf/naglowki.pdf>
- http://archive.endemic.org/spam/sledzenie_5_2004_pl.pdf
- <http://technet.microsoft.com/pl-pl/library/cc737560%28WS.10%29.aspx>
- http://pl.wikipedia.org/wiki/Serwer_poczty_elektronicznej
- http://pl.wikipedia.org/wiki/Skrzynka_poczty_elektronicznej
- http://pl.wikipedia.org/wiki/Klient_poczty_elektronicznej
- <http://aipsa.ita.pwr.wroc.pl/~plab/internet/IPv4.html>
- <http://republika.pl/architect/ipv4.html>
- <http://republika.pl/kasprz/index.htm>
- <http://republika.pl/kmis/tcpip.htm>

- http://republika.pl/m_moszynski/Inform/tcpip.htm
- <http://dreamnet.help.pl/technologie/tcpip/tcpip.php>
- <http://republika.pl/ckzos/sieci.htm>
- <http://www.ampr.torun.pl/packet/tcpip/node1.html>
- <http://republika.pl/fuzzy5/>
- <http://www.waldemar wielki.republika.pl/sieci.html>
- http://republika.pl/dundy/po_co.htm

Możliwości uzyskiwania oraz analizy danych gromadzonych przez przewoźników lotniczych dotyczących przelotu pasażera (PNR)

Wprowadzenie

Artykuł poświęcony jest opisowi specyficznej bazy danych, której oficjalna nazwa to Passenger Name Record (PNR), a która zawiera informacje dotyczące pasażera lub grupy pasażerów podróżujących transportem lotniczym. Straż Graniczna wykorzystuje dane PNR przekazywane z wyprzedzeniem przez przewoźników lotniczych, w trakcie realizacji zadań służbowych, do których należą w szczególności: ochrona granicy państwowej¹ oraz kontrola ruchu granicznego². Informacje zawarte w danych PNR, stanowią cenne źródło wiarygodnych i aktualnych informacji oraz mogą być wykorzystane jako materiał dowodowy również przez inne uprawnione instytucje.

Cel gromadzenia danych PNR

Celem przetwarzania danych PNR jest wykrywanie i zwalczanie przestępstw o charakterze terrorystycznym i innych przestępstw lub przestępstw skarbowych oraz zapobieganie im i ściganie ich sprawców na podstawie ustawy z dnia 9 maja 2018r. o przetwarzaniu danych dotyczących przelotu pasażera (Dz. U. z 2019 r. poz.1783 z późn. zm.) zwana dalej: ustawą PNR. Ustawa jest następstwem dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania (Dz. U. UE z 2016 r. poz. L 119/132 CELEX numer: 32016L0681)³.

Dane PNR obejmują informacje gromadzone podczas dokonania rezerwacji oraz realizacji przewozu lotniczego. Lot PNR oznacza lot „pozaunijny” albo lot „wewnątrzunijny” statku powietrznego wykonującego przewóz lotniczy pasażerów, w tym nieodpłatny, podczas którego następuje przekroczenie granicy państwowej, a start albo lądowanie tego statku następuje na terytorium Rzeczypospolitej Polskiej⁴. System pozyskiwania danych PNR uzupełnia inne narzędzia uprawnionych organów do zwalczania przestępczości transgranicznej.

Straż Graniczna w celu realizacji ustawowych zadań może przetwarzać dane osobowe w rozumieniu ustawy z dnia 14 grudnia 2018r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125), bez wiedzy i zgody osoby, której dane dotyczą (art. 9 ust. 1 lit. a ustawy z dnia 12 października 1990 r. o Straży Granicznej).

¹ Ochrona granicy państwowej (na lądzie i na morzu) – czynności polegające głównie na eliminowaniu przypadków bezprawnego jej przekraczania przez osoby, środki transportu.

² Kontrola ruchu granicznego, kontrola graniczna (realizowana w przejściach granicznych) – czynności związane z weryfikacją legalności przekraczania granicy państwowej, spełnienia zasad wjazdu i pobytu.

³ <https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:32016L0681> [dostęp: 10.11.2025 r.].

⁴ Ustawa z dnia 9 lipca 2025 r. o zmianie ustawy o przetwarzaniu danych dotyczących przelotu pasażera (Dz. U. z 2025 r. poz.1179).

Zakres danych PNR

Dane PNR to dane dotyczące przelotu pasażera, w tym dane osobowe. Przewoźnik lotniczy gromadzi dane PNR w związku z prowadzeniem działalności gospodarczej w celu dokonania rezerwacji lub realizacji lotu w ramach przewozu lotniczego.

Gromadzone dane PNR zawierają⁵:

1. datę dokonania rezerwacji lub wystawienia biletu lotniczego,
2. datę planowanego przelotu,
3. imię i nazwisko pasażera,
4. adres, numer telefonu i adres e-mail pasażera,
5. informacje dotyczące płatności za bilet, obejmujące m.in. numer karty płatniczej, numery rachunków bankowych nadawcy przelewu, imię, nazwisko lub nazwę nadawcy oraz kwotę i walutę,
6. trasę przelotu pasażera,
7. informacje o programach lojalnościowych,
8. nazwę, numer telefonu, adres e-mail i adres biura podróży lub agencji turystycznej,
9. dane o statusie podróży pasażera,
10. informacje dotyczące osoby małoletniej podróżującej bez opieki statkiem powietrznym,
11. numer biletu, datę jego wystawienia,
12. numer miejsca na pokładzie statku powietrznego i inne informacje dotyczące tego miejsca,
13. informacje dotyczące liczby, rodzaju i wagi bagażu,
14. liczbę oraz imiona i nazwiska innych pasażerów dotyczących dokonanej rezerwacji,
15. szczegółowe informacje dotyczące pasażera przekazane przez przewoźnika lotniczego przed podróżą (zwane też danymi API) obejmujące:
 - a) rodzaj, numer, kraj wydania i datę ważności dokumentu tożsamości,
 - b) obywatelstwo,
 - c) imię i nazwisko,
 - d) płeć,
 - e) datę urodzenia,
 - f) nazwę linii lotniczych, numer lotu oraz datę i godzinę startu/lądowania statku powietrznego,
 - g) nazwę portu lotniczego, w którym nastąpił start/lądowanie,
16. wszelkie informacje o zmianach w przesłanych wcześniej ww. danych PNR.

Przewoźnik lotniczy, który organizuje lot PNR, przekazuje ww. dane do Krajowej Jednostki do spraw Informacji o Pasażerach (JIP) zgodnie z art. 5 ustawy PNR. W Polsce JIP funkcjonuje w strukturze Komendy Głównej Straży Granicznej.

⁵ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/681 ZAŁĄCZNIK I „Dane dotyczące przelotu pasażera zbierane przez przewoźników lotniczych”.
<https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:32016L0681> [dostęp: 10.11.2025 r.].

Dane kontaktowe:

Krajowa Jednostka do Spraw Informacji o Pasażerach⁶

al. Niepodległości 100

02-514 Warszawa

E-mail: piu.pl@strazgraniczna.pl

Tel: 225135500 **całodobowo!**

Fax. 225004600-01 **całodobowo!**

Elektroniczna skrzynka podawcza (ePUAP) – /KGSG/pnr

Również inne organy uprawnione do występowania o przekazanie danych PNR lub wyników ich przetwarzania, zostały zobligowane do wyznaczenia punktu kontaktowego właściwego w sprawach przetwarzania danych PNR.

Komendant Główny Policji wyznaczył punkt kontaktowy właściwy w sprawach przetwarzania danych PNR – Sekcję Całodobowej Obsługi Punktu Kontaktowego PNR, która funkcjonuje w ramach Wydziału Administrowania Danymi SIS i VIS Biura Wywiadu i Informacji Kryminalnych Komendy Głównej Policji. Szczegóły funkcjonowania punktu kontaktowego reguluje Zarządzenie nr 64 Komendanta Głównego Policji z dnia 22 listopada 2018r. (Dz. Urz. KGP poz. 123 z późn. zm.).

Dane kontaktowe:

Sekcja Całodobowej Obsługi Punktu Kontaktowego PNR⁷

Wydziału Administrowania Danymi SIS i VIS Biura Wywiadu i Informacji

Kryminalnych Komendy Głównej Policji

ul. Taborowa 33 B 02-699 Warszawa

tel.: 226011450 **całodobowo!**

faks: 226011456 **całodobowo!**

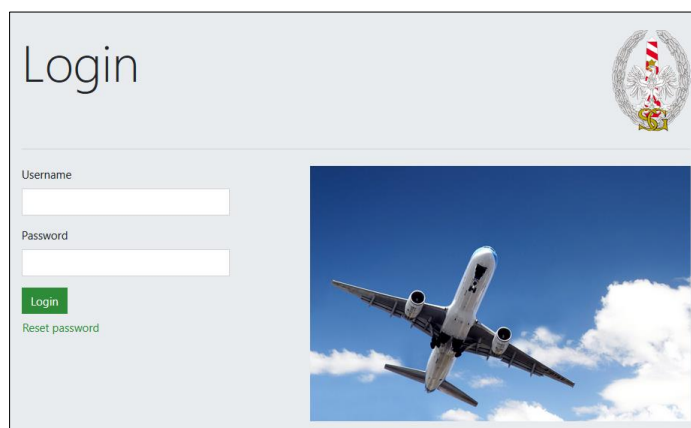
e-mail: kgp.pnr@policja.gov.pl

Portal Przewoźnika Lotniczego jest bezpłatnym kanałem przekazywania danych PNR, udostępnianym i administrowanym przez JIP. To aplikacja w postaci serwisu [www \(https://ksipnr.strazgraniczna.pl\)](http://www.ksipnr.strazgraniczna.pl) umożliwiająca przewoźnikom lotniczym bezpośrednio przysyłanie danych PNR do JIP poprzez ich manualne wprowadzenie bądź import paczki danych do Krajowego Systemu Informatycznego (KSI PNR)⁸.

⁶ <https://www.bip.kgsg.strazgraniczna.pl/s01/passenger-name-record/12410,Passenger-Name-Record-PNR.html> [dostęp: 10.11.2025 r.].

⁷ <https://www.policja.pl/pol/kgp/bwik/aktualnosci-1/biezace-informacje/167808,Dostep-Policji-do-danych-PNR.html> [dostęp: 10.11.2025 r.].

⁸ Instrukcja użytkownika „Portalu Przewoźnika Lotniczego (PPL) ver. 1”, 2020, str. 3.



Fot. 1. Widok strony logowania do Portalu Przewoźnika Lotniczego. Źródło: materiały własne, 2025

Przewoźnicy lotniczy mają obowiązek przekazywania danych PNR do JIP od 48 do 24 godzin przed planowanym rozpoczęciem lotu oraz po zakończeniu odprawy biletowo-bagażowej i wejściu pasażerów na pokład samolotu.

Dane zgromadzone w KSI PNR dostępne są dla uprawnionych służb oraz instytucji porządku publicznego w trybie wnioskowym. Katalog przestępstw w związku z którymi możliwe jest uzyskanie danych PNR zawiera przestępstwa o charakterze terrorystycznym oraz poważne przestępstwa⁹. W odpowiedzi na wniosek i sprawdzenie bazy danych, generowany jest dokument w formie pliku PDF – pismo przewodnie oraz załącznik zawierający wyniki. W przypadku wnioskowania o pełne dane dodatkowo przesyłany jest plik w formacie XML w standardzie PNRGOV¹⁰.

Dane osobowe zgromadzone w systemie KSI PNR lub wyniki ich przetwarzania mogą być przekazywane również na wniosek ze strony:

- JIP innego państwa członkowskiego,
- Europolu,
- państwa trzeciego – pod warunkiem, że jest to konieczne dla realizacji celów określonych w ustawie PNR, organ państwa trzeciego jest właściwy w sprawach wykrywania i zwalczania przestępstw oraz zapobiegania im i ścigania ich sprawców oraz zapewnia ono odpowiedni poziom ochrony przekazywanych danych osobowych (art. 53-57 ustawy PNR).

Dane PNR są przechowywane w KSI PNR przez okres 5 lat od dnia ich wprowadzenia, a po upływie tego okresu podlegają niezwłocznie trwałemu usunięciu. Natomiast po upływie 6 miesięcy od dnia ich wprowadzenia, dane PNR są poddawane depersonalizacji przez uczynienie niewidocznymi te kategorie danych PNR, które mogą służyć do bezpośredniej identyfikacji pasażera (art. 32 ust. 1 i 33 ust. 1 ustawy PNR).

Należy dodać, iż JIP w Polsce jest również uprawniona do pozyskiwania danych PNR i wyników ich przetwarzania od JIP państw członkowskich (JIP PCz), na podstawie wniosku od właściwego organu krajowego.

⁹ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/681 ZAŁĄCZNIK II „Wykaz przestępstw, o których mowa w art. 3 pkt 9” <https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:32016L0681> [dostęp: 10.11.2025 r.].

¹⁰ tamże, str. 4.

Fot. 2. Widok zakładki w KSI PNR dotyczącej wniosku o przekazanie danych

Źródło: materiały własne, 2025

Wniosek o którym mowa można złożyć w formie:

- pisemnej – poprzez przekazanie wypełnionego druku, zawierającego dane ogólne, uzasadnienie oraz szczegółowy zakres danych których dotyczy,
- ustnej – sprawy pilne (konieczne potwierdzenie wniosku w formie pisemnej).

Zakres dostępnych danych PNR

Rodzaje danych PNR o które można wnioskować, dzielimy na dwie grupy:

1. Archiwalne dane PNR czyli informacje, które już zostały zgromadzone w ciągu 5 lat przez:
 - 1.1. JIP w Polsce,
 - 1.2. inne JIP PCz.
2. Dane dotyczące przyszłych lotów czyli informacje o podróżnym, które mogą się pojawić w przyszłości:
 - 2.1. poprzez moduł EZOW – wpis do Ewidencji Zleceń Organów Właściwych,
 - 2.2. na podstawie kryteriów – typowanie, profilowanie.

JIP w Polsce

Wzór wniosku o dane archiwalne kierowany do JIP w Polsce przedstawiono w załączniku nr 1¹¹. Należy pamiętać, że przewoźnicy lotniczy często nie przesyłają danych takich jak płeć, data urodzenia (DOB) lub numer dokumentu. Dlatego często koniecznym okazuje się odpytanie bazy PNR po danych zbieżnych – bez podawania DOB. Przykład poprawnego wypełnienia tabeli SZCZEGÓŁOWY ZAKRES DANYCH w zależności od oczekiwanego wyniku, przedstawiono poniżej:

¹¹ Załącznik do zarządzenia nr 64 dla Policji <https://sip.lex.pl/akty-prawne/dzienniki-resortowe/dostep-policji-do-danych-dotyczacych-przelotu-pasazera-pnr-35558822> [dostęp 10.11.2025 r.].

A. W celu uzyskania danych PNR **identycznych** jak we wniosku:

ZAKRES	WARUNEK	OPERATOR	WARTOŚĆ
Dane podstawowe	Imię	zawiera	Jan
Dane podstawowe	Nazwisko	równy	Nowak
Dane podstawowe	Data urodzenia	równy	1991-01-01

Tabela nr 1. Zakres danych PNR identycznych jak we wniosku

Źródło: materiały własne, 2025

B. W celu uzyskania danych PNR **identycznych** jak we wniosku oraz danych **zbieżnych**:

ZAKRES	WARUNEK	OPERATOR	WARTOŚĆ
Dane podstawowe	Imię	zawiera	Jan
Dane podstawowe	Nazwisko	równy	Nowak

Tabela nr 2. Zakres danych PNR identycznych oraz danych zbieżnych

Źródło: materiały własne, 2025

Należy pamiętać, iż:

- w przypadku wnioskowania o zakres danych powyżej 6 miesięcy od dnia wniosku, wymagana jest zgoda prokuratora lub sądu potwierdzająca, że warunki ujawnienia zdepersonalizowanych danych PNR zostały w danym przypadku spełnione,
- przy danych zbieżnych (ppkt. B) istnieje ryzyko, że mogą one należeć do innej osoby niż objętej wnioskiem i wymagana będzie dodatkowa weryfikacja,
- w celu uzyskania wszystkich danych zaleca się wnioskowanie o przekazanie danych w formacie XML.

JIP PCz

Wzór wniosku o dane archiwalne kierowany do JIP PCz przedstawiono w załączniku nr 2¹². Istotnym elementem wniosku jest załącznik w formie arkusza Excel (formularz PNR Request.xlsx), który zawiera wszystkie dostępne warianty zapytania.

PNR Request		SIENA Case Reference	Section incomplete
		National Case Reference	
		Operation Name/Reference	
		Confidentiality	
** Completion note - GREY FIELDS are MANDATORY & YELLOW FIELDS are OPTIONAL **			
** Completion note - any personal data of PIU/NCA staff should be inserted into "Personal communication" field in SIENA **			
** Completion check - SECTIONS INCOMPLETE, please review the remaining GREY fields **			
1. REQUESTED BY:		2. AUTHORISED BY: Section incomplete	
Request - Passenger Information Unit		Authorisation - Passenger Information Unit	
Request - Date and Time		Authorisation - Date and Time	
Request - Operational Phone Number		Authorisation - Independent Authority	
Request - Operational E-mail Address		Authorisation - Date and Time	
Request - On behalf of National Competent Authority		Authorisation - Reference Number	
3. REQUESTED FROM:		Section incomplete	
Passenger Information Units:		EUROPOL's Travel Intelligence:	
☐ Austria ☐ Estonia ☐ Ireland ☐ Netherlands ☐ Spain ☐ Belgium ☐ Finland ☐ Italy ☐ Poland ☐ Sweden ☐ Bulgaria ☐ France ☐ Latvia ☐ Portugal ☐ Other ☐ Croatia ☐ Germany ☐ Lithuania ☐ Romania ☐ Cyprus ☐ Greece ☐ Luxembourg ☐ Slovakia ☐ Czech Republic ☐ Hungary ☐ Malta ☐ Slovenia		☐ Hit / No hit (no storage) ☐ Full information (storage) If any of the above boxes has been selected, the data from this request will be searched against Europol data. By "Hit/No Hit" you will receive only hit/no hit notification; data will NOT be stored. By "Full information", you will also receive criminal data (available to Europol) linked to the hit; data will be stored (for reporting also potential future hits). See more guideline in instructions tab!	

Fot. 3. Załącznik do wniosku o przekazanie danych PNR przez JIP PCz (formularz PNR Request.xlsx). Źródło: materiały własne, 2025

¹² Załącznik do zarządzenia nr 64 dla Policji <https://sip.lex.pl/akty-prawne/dzienniki-resortowe/dostep-policji-do-danych-dotyczacych-przelotu-pasazera-pnr-35558822> [dostęp 10.11.2025 r.].

Możliwe jest wyszukiwanie danych metodą dopasowań dokładnych (exact search only) lub dopasowań rozmytych (wider search). Można również zawnioskować o wpis danych na tzw. listę obiektów obserwowanych (watchlist) w innych krajach członkowskich. Wpis taki może być ważny przez okres nie dłuższy niż 6 miesięcy z możliwością przedłużenia. Kraje: Austria, Belgia, Bułgaria, Niemcy i Irlandia obecnie nie respektują takiego wpisu od innych państw członkowskich UE.

W poniższej tabeli przedstawiono wykaz państw członkowskich UE, które postanowiły zastosować Dyrektywę UE 2016/681 do lotów zewnętrznych (poza UE) i wewnętrznych (wewnątrz UE). Należy zauważyć, iż Dania i Szwajcaria są obecnie traktowane jako kraje trzecie i JIP nie realizuje wniosków do tych krajów.

Kraje które gromadzą dane PNR z lotów zewnętrznych (poza UE)	Kraje które gromadzą dane PNR z lotów wewnętrznych (wewnątrz UE)
Austria	-----
Belgia	Belgia
Bułgaria	Bułgaria
Chorwacja	Chorwacja
Cypr	Cypr
Czechy	Czechy
Estonia	Estonia
Finlandia	Finlandia
Francja	Francja
Grecja	Grecja
Hiszpania	Hiszpania
Niderlandy	Niderlandy
Irlandia	-----
Litwa	Litwa
Luksemburg	Luksemburg
Łotwa	Łotwa
Malta	Malta
Niemcy	Niemcy
Polska	Polska
Portugalia	Portugalia
Rumunia	Rumunia
Słowacja	Słowacja
Słowenia	Słowenia
Szwecja	Szwecja
Węgry	Węgry
Włochy	Włochy

Tabela nr 3. Wykaz państw członkowskich UE które gromadzą dane PNR

Źródło: materiały własne, 2025

Wzór wniosku do JIP o dane zgromadzone przez JIP Wielkiej Brytanii przedstawiono w załączniku nr 3¹³.

Należy zaznaczyć, iż odpowiedzi z zagranicy przesyłane są na bieżąco do wnioskodawcy, dlatego też przy kilku adresatach (kilku JIP PCz) należy mieć świadomość, że jednego dnia można dostać odpowiedź np. z JIP Niemcy, drugiego z JIP Hiszpania, natomiast z JIP Włochy dopiero za tydzień. Dodatkowo odpowiedzi z JIP PCz mogą być wysłane w całości (full answer) lub w części (partial answer), czyli wysyłając do JIP Belgia możemy dzisiaj otrzymać częściową odpowiedź, a za tydzień dalszą jej część (która np. dotyczyła danych zdepersonalizowanych i wymagała otrzymania zgody tamtejszego prokuratora).

W następstwie uznania wyroku Trybunału Sprawiedliwości Unii Europejskiej (TSUE) w sprawie C-817/19¹⁴ przez Niemcy i Niderlandy, kraje te wprowadziły ograniczenia w udostępnianiu swoich danych PNR:

- Niemcy: z systemu PNR zostały usunięte wszystkie dane PNR przechowywane przez ponad sześć miesięcy, a w najbliższej przyszłości zostanie ograniczona ilość przechowywanych danych PNR z tras wewnątrzunijnych. Ponadto wskazano, że sąd w Wiesbaden będzie organem odpowiedzialnym za nadzorowanie wszystkich indywidualnych wniosków o dostęp do danych PNR przechowywanych w niemieckich systemach, dlatego udzielenie odpowiedzi może zająć więcej czasu niż dotychczas. Każdy wniosek będzie musiał mieć szczegółowe uzasadnienie w zakresie opisu przypadku, konieczności i proporcjonalności oraz powiązania sprawy/pasażera z Niemcami.
- Niderlandy: okres przechowywania danych PNR został zmieniony z 5 do 3 lat. Dane PNR starsze niż 3 lata zostają usunięte, chyba że w ciągu trzech lat pojawi się związek między konkretnymi danymi PNR a terroryzmem lub poważną przestępczością. Ponadto ujawnienie danych PNR będzie podlegało wcześniejszemu przeglądowi przez prokuratora, co może oznaczać dłuższy okres oczekiwania na odpowiedź z PIU Niderlandy i bardziej szczegółowe uzasadnienia wniosków.

EZOW

Ewidencja Zleceń Organów Właściwych (EZOW) to zbiór zainteresowań osobami, zasilany wpisami Właściwych Organów, które ze względu na obostrzenia nie kwalifikują się do wpisu do innych krajowych i międzynarodowych baz poszukiwawczych (np. KSIP, EZ, SIS, INTERPOL).

Jedyną formą zlecenia jest tu „zamówienie” przez wnioskodawcę informacji o planowanej aktywności osoby w ruchu lotniczym. Jeśli osoba wpisana w EZOW wystąpi w komunikacji PNR, wnioskodawca otrzyma od JIP informację o tym fakcie, zawierającą czas i miejsce planowanego przekroczenia granicy drogą lotniczą. Wpis w EZOW dotyczy wyłącznie zlecenia informowania wnioskodawcy a zatem tylko jednostka zlecająca otrzyma informację i tylko ona może na nią zareagować.

¹³ Załącznik do zarządzenia nr 64 dla Policji <https://sip.lex.pl/akty-prawne/dzienniki-resortowe/dostep-policji-do-danych-dotyczacych-przelotu-pasazera-pnr-35558822> [dostęp 10.11.2025 r.].

¹⁴ <https://legalis.pl/novelizacja-ustawy-o-przetwarzaniu-danych-dotyczacych-przelotu-pasazera/> [dostęp 10.11.2025 r.].

Wzór wniosku kierowany do JIP o dodanie wpisu do bazy EZOW przedstawiono w załączniku nr 4. Istnieje również możliwość dokonania modyfikacji wpisu do bazy EZOW a także możliwość usunięcia wpisu do bazy EZOW.

Data ważności zlecenia wpisu do bazy EZOW uzależniona jest od oczekiwania ze strony wnioskującego co do dokładności danych identyfikacyjnych osoby a konkretnie daty urodzenia (DOB). Istnieją dwie opcje dla prawidłowej realizacji wniosku:

- z datą urodzenia (DOB) **wpis ważny do 6 miesięcy**,
- bez daty urodzenia (uwaga wpisana w uzasadnieniu: „bez DOB”) **wpis ważny do 2 tygodni** (z możliwością przedłużenia).

Warianty, w których system KSI PNR wygeneruje pozytywne wyniki sprawdzeń dla poniższego wpisu w bazie EZOW przedstawiono w poniższej tabeli:

- imię: KATARZYNA nazwisko: KWIATKOWSKA DOB: 12.12.1965 UWAGA: bez DOB

Lp.	Imię	Nazwisko	Data urodzenia DOB	Trafienie zakończone przestaniem powiadomienia
1.	KATARZYNA	KWIATKOWSKA	12.12.1965	TAK
2.	KATARZYNA ANNA	KWIATKOWSKA	12.12.1965	TAK
3.	ANNA KATARZYNA	KWIATKOWSKA	12.12.1965	TAK
4.	KATARZYNA	KWIATKOWSKA		TAK
5.	KATARZYNA ANNA	KWIATKOWSKA		TAK
6.	KATARZYNAS	KWIATKOWSKA		TAK
7.	KATARZYNAMRS	KWIATKOWSKA		TAK
8.	KATARZYNA	KWIATKOWSKA	10.12.1965	NIE
9.	ANNA	KWIATKOWSKA	12.12.1965	NIE
10.	KATARZYNA	KWIATKOWSKA KWIAT	12.12.1965	NIE

Tabela nr 4. Warianty odpowiedzi z systemu KSI PNR. Źródło: materiały własne, 2025

W odpowiedzi na ww. wniosek dotyczący osoby, podając jej imię, nazwisko i datę urodzenia (DOB) oraz zaznaczając w uzasadnieniu „bez DOB” otrzymamy dodatkowo odpowiedzi z wiersza 4, 5, 6 i 7. Jak widać dla imion wyszukiwarka stosuje wariant rozmyty – wystarczy gdy jedno z imion wpisu do EZOW jest identyczne z danymi PNR a otrzymamy trafienie. Nie otrzymamy natomiast odpowiedzi z wiersza 10 (nie uwzględnienie nazwiska dwuczłonowego KWIATKOWSKA KWIAT), ponieważ dla nazwisk system KSI PNR generuje wyniki wyłącznie gdy wpis do EZOW jest identyczny (również kolejność) z danymi PNR.

Należy pamiętać, iż wpis do EZOW daje możliwość uzyskania informacji:

- dotyczących osób poruszających się tylko w ruchu lotniczym i przekraczających granicę państwową w porcie lotniczym,
- zawierającą czas i miejsce planowanego przekroczenia granicy,
- pod warunkiem poprawnego wpisu danych osobowych do bazy EZOW (uwzględnienia wszystkich wariantów).

Typowanie – profilowanie

JIP przetwarzając dane PNR, dokonuje w sposób zautomatyzowany sprawdzeń pasażerów lotów PNR w celu identyfikacji osób, które wymagają podjęcia dalszych działań przez właściwe organy określone w art. 36 ustawy PNR.

W przypadku uzyskania pozytywnego wyniku sprawdzenia podlega on indywidualnej ocenie, w sposób niezautomatyzowany, w celu ustalenia, czy dane PNR lub wyniki ich przetwarzania podlegają niezwłocznemu przekazaniu przez JIP właściwemu organowi (art. 19 i 20 ustawy PNR).

Profil tworzy się na podstawie:

- I. Analizy konkretnych archiwalnych przypadków, np. zatrzymań osób oraz szczegółów ich rezerwacji lotniczych (kategorii danych PNR), trasy przemieszczania się, rodzaju i nr dokumentu podróży, formy płatności, danych osoby opłacającej rezerwację, numeru telefonu, adresu mailowego, rodzaju bagażu itp.
- II. Analizy ustalonych zachowań (modus operandi) przestępców, znanych organom ścigania; poprzez stworzenie profilu, tj. kryteriów przetwarzania danych PNR (czyli odpowiednio dobranych kategorii danych PNR), można próbować identyfikować inne osoby wykazujące w ruchu lotniczym podobne przestępcze zachowania.

Wzór wniosku kierowany do JIP o ustalenie/aktualizację kryteriów przetwarzania danych PNR przedstawiono w załączniku nr 5. Istnieje również możliwość usunięcia kryteriów przetwarzania danych PNR.

Zasady tworzenia kryteriów przetwarzania danych PNR¹⁵:

- kryteria tworzone są z co najmniej 5 a maksymalnie z 20 elementów kategorii danych PNR,
- każdemu elementowi należy przypisać tzw. wagę (wyrażoną w %); minimalna wartość/waga jednego elementu kategorii danych PNR wynosi 5% a maksymalna 20%; suma wag zawsze musi wynieść 100%,
- kryteria przetwarzania danych PNR muszą zawierać tzw. minimalną wagę prezentowania trafienia (wyrażoną w %) tj. wartość przy której system KSI PNR dokonując automatycznych sprawdzeń danych PNR wskaże pozytywny wynik (zbieżność lub identyczność danych PNR z ustalonymi kryteriami); wartość minimalnej wagi prezentowania trafienia musi wynosić 70% a maksymalnej 100%,
- kryteria mogą obowiązywać maksymalnie 6 miesięcy,
- ustalone kryteria mogą być aktualizowane (na okres nie dłuższy niż kolejne 6 miesięcy) lub usunięte.

Czynności po uzyskaniu trafienia na podstawie zdefiniowanego kryterium:

- po trafieniu osoby spełniającej parametry kryteriów (zgodność danych rezerwacyjnych osoby z zadanymi parametrami musi uzyskać określoną wagę minimalną) wynik przesyłany jest do wnioskodawcy,
- w szczególnych sytuacjach wynik może być przesłany również do Placówki Straży Granicznej – lotniczego przejścia granicznego, na terenie którego osoba może się pojawić, jednak wymaga to wcześniejszych uzgodnień wnioskodawcy i SG.

¹⁵ „Udostępnianie danych PNR – wnioskowanie, technika i alia, dobre praktyki” materiały szkoleniowe ZOŚ, s. 55.

Wskazówki dotyczące tworzenia kryteriów przetwarzania danych PNR¹⁶:

- a) ustalając kryteria należy wiedzieć czego szukamy,
- b) wskazane jest by kryteria „odpowiadały” na kilka następujących pytań:
 - kto – płeć, wiek, obywatelstwo, kraj wydania dokumentu podróży; należy pamiętać, że w komunikacie PNR osoba może występować w kilku rolach – jako pasażer, osoba dokonująca rezerwacji, płacąca za bilet (sponsor),
 - gdzie, skąd/dokąd – kraj lub lotnisko przylotu i odlotu, gdzie dokonano rezerwacji,
 - kiedy – konkretne daty lub przybliżone okresy przylotów i odlotów bądź dokonania rezerwacji,
 - jak, w jaki sposób – jaką linią lotniczą podróżowano, w jaki sposób zapłacono za bilet, czy skorzystano z usług biura podróży, jakim dokumentem legitymował się podróżny itp.,
 - jakie dane kontaktowe podano – adres e-mail, numer telefonu, adres pobytu/za-mieszkania,
- c) ustalamy kryteria tylko wtedy, gdy jest taka potrzeba oraz będzie czas, siły i środki do tego, by zweryfikować otrzymane powiadomienia i właściwie je wykorzystać,
- d) ustalamy kryteria w oparciu o analizę materiałów operacyjnych, prasowych dotyczących podobnych zdarzeń; szukamy wspólnego mianownika dla tych przypadków, ustalamy modus operandi w ruchu lotniczym, typujemy i przewidujemy,
- e) pamiętajmy, że informacja uzyskana z powiadomienia z komunikatu PNR jest tylko zapowiedzią udziału osoby w ruchu lotniczym – przesłana na kilkadziesiąt godzin przed lotem, który może nie odbyć się lub osoba ta może nie wsiąść na pokład samolotu,
- f) przed ustaleniem kryteriów dokonajmy przeglądu sytuacji w Polsce, Europie czy na świecie; zwróćmy uwagę czy w najbliższym czasie nie są organizowane międzynarodowe imprezy masowe oraz czy nie mają miejsce zdarzenia losowe, które mogą mieć wpływ na nagły wzrost lub spadek liczby pasażerów w ruchu lotniczym,
- g) jeżeli ustalimy kryteria a mamy wiedzę o czynnikach, które mogą na nie znacząco wpłynąć, reagujemy poprzez aktualizację kryteriów; w ten sposób unikamy otrzymywania dużej ilości trafień „fałszywie pozytywnych”.

Prezentacja i analiza danych PNR

Jak wspomniano wcześniej w odpowiedzi na wniosek o pełne dane PNR, generowany jest załącznik w formacie XML w standardzie PNRGOV zawierający kompletne wyniki. W celu dokonania konwersji pliku XML na bardziej czytelny format prezentacji danych (.PDF, .XLSX), możemy skorzystać z programu stworzonego przez AGH w Krakowie o nazwie PNR Analizer ver. 3.0 (wcześniej FinLink Konwerter)¹⁷.

Aplikacja umożliwia przekonwertowanie danych z dostępnych oryginalnie formatów XML do postaci pozwalającej na ich prezentację a także umożliwia ich analizę. Dane są filtrowane i agregowane oraz prezentowane w formie szeregu zestawień przeznaczonych dla typowych zastosowań i co równie ważne w postaci łatwo czytelnej dla użytkownika.

¹⁶ „Udostępnianie danych PNR – wnioskowanie, technika, dobre praktyki” materiały szkoleniowe ZOŚ, s. 79.

¹⁷ Aplikacja do pobrania dla uprawnionych instytucji po wcześniejszej rejestracji konta użytkownika na stronie <https://finlink.agh.edu.pl/> [dostęp 10.11.2025r.]

Z perspektywy analizy danych PNR Analyzer pozwala na łatwiejsze wyciąganie wniosków, a także chroni przed błędami w interpretacji danych.

The screenshot displays the 'PNR Analyzer ver. 3.0.0' application window. On the left is a dark blue sidebar with navigation options: 'Wyszukiwanie danych', 'Wybór plików', 'Wyszukiwanie danych', and 'Katalog teczek'. The main area is titled 'Parametry wyszukiwania' and contains two sections: 'Dane pasażera' and 'Dane lotu'. The 'Dane pasażera' section includes input fields for 'Nazwisko', 'Imię', 'Data urodzenia' (with a date picker), 'Telefon', 'E-mail', 'Numer dokumentu', 'Płeć', 'Obywatelstwo', 'Rodzaj płatności', and 'Sponsor'. The 'Dane lotu' section includes dropdowns for 'Kraj odlotu', 'Kod lotniska', 'Nazwa lotniska odlotu', 'Data odlotu' (with a date picker), 'Numer lotu', 'Kod przewoźnika', 'Nazwa przewoźnika', 'Kraj przylotu', 'Kod lotniska', 'Nazwa lotniska przylotu', and 'Data przylotu' (with a date picker). Below these sections are buttons for 'Wyszukaj', 'Wyczyść', and 'Mniej parametrów'. Underneath is a 'Lista pasażerów' section with a table of search results. The table has columns: 'Lp.', 'Nazwisko', 'Imię', 'Data urodzenia', 'Nr dokumentu', 'Lotnisko odlotu', 'Data odlotu', 'Lotnisko przylotu', 'Data przylotu', 'Nr rezerwacji', and 'Przewoźnik/Nr lotu'. The first four rows show results for 'TYPROWICZ Tomasz, Tomasz Mr' with flight details to and from Munich. At the bottom of the table, there is a summary: 'Liczba zaimportowanych pozycji: 12 | Liczba dopasowań: 12 | Liczba wybranych pozycji: 4'. A 'GENERUJ RAPORT' button is located at the bottom right of the interface.

Fot. 4. Widok strony wyszukiwania danych aplikacji PNR Analyzer. Źródło: materiały własne, 2025

Aplikacja korzysta m.in. z zewnętrznego słownika, utworzonego w projekcie OpenFlights (airports.dat), dostarczającego informacji na temat stref czasowych oraz długości i szerokości geograficznej lotnisk, tak aby wyświetlać daty przylotów, odlotów oraz odprawy granicznej w polskiej strefie czasowej.

Aplikacja po uruchomieniu prosi o wybranie pliku/folderu z danymi PNR i od razu umożliwia ich przeglądanie oraz przeszukiwanie. Mamy również możliwość wybrania formatu raportu generowanego na podstawie wybranych danych. Forma i zawartość dostępnych raportów została zdefiniowana w odpowiedzi na potrzeby użytkowników w codziennej pracy z danymi PNR. Istnieje również opcja katalogowania rekordów poprzez grupowanie wybranych rekordów do definiowanych teczek.

Rodzaje dostępnych szablonów raportów:

- Raport skrócony to raport utworzony na potrzeby wydruku podstawowych danych zawartych w pliku z odpowiedzią z bazy KSI PNR, nie wszystkie dane są prezentowane.
- Raport dla analityków to raport utworzony na potrzeby zespołów analitycznych Straży Granicznej i Policji. W założeniu ma zawierać możliwie szeroki zestaw danych z pliku PNR w formacie umożliwiającym ich dalszą obróbkę przez użytkowników. Ma umożliwiać przetwarzanie większej ilości danych PNR i dalszą ich analizę.
- Wypis z pliku.xml dla Policji to raport operacyjny na potrzeby Sekcji Całodobowej Obsługi Punktu Kontaktowego PNR Komendy Głównej Policji. Jest załącznikiem do wniosków o udostępnienie danych do celów operacyjnych, razem z plikiem.xml pozyskanym z systemu KSI PNR.

- Dossier Straży Granicznej to raport operacyjny dla Straży Granicznej, utworzony na potrzeby komunikacji wewnątrz służby w kraju i w ramach współpracy z jednostkami służb granicznych na terenie Unii Europejskiej. Z założenia jest to dokument pozwalający na szybki i przejrzysty wgląd w dane pasażera i współpasażerów, lotów i rezerwacji.
- Raport dla Europolu to raport stworzony na potrzeby wymiany danych pomiędzy Strażą Graniczną a Europolem. Jest zgodny z przyjętym protokołem komunikacji opartym o formalne zapytanie i odpowiedź. Zakres danych w raporcie jest zgodny ze specyfiką wymaganej formalnej odpowiedzi.
- Raport dla Linka to raport stworzony na potrzeby ułatwienia importu danych PNR do środowiska analitycznego Link.

Podsumowanie

Każdy przewoźnik lotniczy, który wykonuje lot PNR (lot, w którym przewozi się pasażerów za wynagrodzeniem np. loty nierozkładowe czy taksówka powietrzna) podczas którego następuje przekroczenie granicy państwowej, a start lub lądowanie następuje na terytorium Polski ma obowiązek przekazywania do JIP danych PNR. Również realizowanie tzw. „lotów tranzytowych”, wymaga przekazania danych PNR zarówno wówczas, gdy pasażerowie podczas postoju statku powietrznego na terytorium RP opuszczają pokład, jak i wówczas, gdy pasażerowie nie opuszczają pokładu statku powietrznego. Przewoźnik lotniczy nie odpowiada natomiast za błędne informacje stanowiące dane PNR podawane przez pasażerów w trakcie dokonywania przez nich rezerwacji lotu¹⁸.

Aktualnie do polskiej bazy KSI PNR podłączonych jest blisko 500 przewoźników lotniczych co oznacza, że do bazy trafiają dane 99,9 % pasażerów. Jednak od dnia wejścia w życie ustawy PNR odnotowano 109897 lotów, w przypadku których obowiązek przekazania danych nie został dopełniony (stan na listopad 2024)¹⁹.

Co możemy zatem ustalić wykorzystując dane PNR:

- potwierdzić fakt wjazdu lub opuszczenia przez osobę terytorium RP lub innego PCz drogą lotniczą,
- ustalić trasy przemieszczania się osób będących w zainteresowaniu,
- ustalić inne osoby lub potwierdzić ich powiązania z osobami będącymi w zainteresowaniu (wspólne rezerwacje, płatności za lot – sponsor),
- ustalić aktualne dane teleadresowe osób pozostających w zainteresowaniu,
- typować osoby i ustalać ich tożsamość poprzez stosowanie kryteriów oraz kierowanie wniosków o przekazanie danych PNR,
- uzyskać z dwudniowym wyprzedzeniem (48 h) informacje o planowanym zamiarze oraz czasie i miejscu przekroczenia granicy przez daną osobę (EZOW),
- poszerzyć wiedzę operacyjną o dane zgromadzone przez inne państwa UE,
- uzyskać materiał dowodowy w okresie do 5 lat od dnia złożenia wniosku o udostępnienie.

Przykładem wykorzystania danych PNR niech będzie ich użycie w szeroko zakrojonej operacji transgranicznej „Moby Dick”, przeciwko oszustwom związanym z wyłudzeniem podatku

¹⁸ „Najczęściej zadawane pytania – Frequently Asked Questions” [dostęp: 10.11.2025 r.].

¹⁹ Briss K., Śliwoska A., 2024, s. 20.

VAT na kwotę 520 mln euro²⁰. Europejska Prokuratura przy wsparciu Europolu dokonała porównania informacji o przelocie pasażera dotyczących ponad 45 osób objętych dochodzeniem w celu identyfikacji powiązań. W wyniku analizy otrzymanych danych wydano nakazy zatrzymania 43 podejrzanych. Postępowania wyjaśniające trwają w kilku krajach UE, w tym w Bułgarii, Chorwacji, na Cyprze, w Czechach, we Włoszech, Luksemburgu, Holandii, na Słowacji i w Hiszpanii, a także w krajach spoza UE. W sumie śledztwo dotyczy 200 osób i ponad 400 firm.

Zbieranie i przetwarzanie danych o pasażerach lotniczych jest cennym narzędziem, które może w istotny sposób przelożyć się na zwiększenie poziomu bezpieczeństwa na terytorium państw członkowskich UE. Jednocześnie dzięki zastosowaniu ograniczeń polegających na określeniu celów przetwarzania i obowiązków związanych z anonimizacją i usuwaniem danych – ogranicza się możliwość naruszeń związanych z przetwarzaniem danych osobowych.

Bibliografia

1. Straż Graniczna, 2020, „Portal Przewoźnika Lotniczego – aplikacja Straży Granicznej do przekazywania danych PNR ver. 1”,
<https://www.bip.kgsg.strazgraniczna.pl/s01/passenger-name-record/12410,Passenger-Name-Record-PNR.html> [dostęp: 10.11.2025 r.].
2. Straż Graniczna, 2020, „Najczęściej zadawane pytania – Frequently Asked Questions”,
<https://www.bip.kgsg.strazgraniczna.pl/s01/passenger-name-record/12410,Passenger-Name-Record-PNR.html> [dostęp: 10.11.2025 r.].
3. Straż Graniczna ZOŚ, 2024, „Udostępnianie danych PNR – wnioskowanie, technikalnia, dobre praktyki” – materiały szkoleniowe.
4. Briss K., Śliwoska A., 2024, „Przetwarzanie danych pasażerów lotniczych. Aktualne problemy prawne w kontekście ochrony danych osobowych i bezpieczeństwa lotniczego”, Krajowa Konferencja Bezpieczeństwa w Lotnictwie Cywilnym Warszawa 21–22 listopada 2024, <https://ulc.gov.pl/> [dostęp: 10.11.2025 r.].
5. Ustawa z dnia 9 maja 2018 r. o przetwarzaniu danych dotyczących przelotu pasażera (Dz. U. z 2019 r. poz.1783 z późn. zm.).
6. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania (Dz. U. UE z 2016 r. poz. L 119/132 CELEX numer: 32016L0681).
7. Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125).
8. Ustawa z dnia 9 lipca 2025 r. o zmianie ustawy o przetwarzaniu danych dotyczących przelotu pasażera (Dz. U. z 2025 r. poz.1179).
9. Ustawa z dnia 12.10.1990 r. o Straży Granicznej (Dz.U.2024.0.915 t.j.).
10. Zarządzenie nr 64 Komendanta Głównego Policji z dnia 22 listopada 2018r. (Dz. Urz. KGP poz. 123 z późn. zm.).

²⁰ <https://www.europol.europa.eu/media-press/newsroom/news/europol-supports-eppo-led-investigation-eur-520-million-vat-fraud-involving-mafia-networks> [dostęp: 10.12.2025 r.]

.....
(miejscowość i data)

.....
Pieczęć wnioskującego organu

Numer pisma WO

ID KSI PNR

**KRAJOWA JEDNOSTKA DO SPRAW
INFORMACJI O PASAŻERACH**

**WNIOSEK O PRZEKAZANIE DANYCH PNR/
POTWIERDZENIE WNIOSKU ZŁOŻONEGO W FORMIE USTNEJ***

Na podstawie art. 21 ustawy z dnia 9 maja 2018r. o przetwarzaniu danych dotyczących przelotu pasażera (Dz. U. 2022 poz. 1441) wnoszę o przekazanie danych PNR

☐ Złożenie wniosku

☐ Potwierdzenie wniosku złożonego w formie ustnej nr
(ID KSI PNR)

DANE OGÓLNE:

1. Oznaczenie sprawy, w której dane PNR lub wyniki ich przetwarzania będą wykorzystywane:

2. Określenie przestępstwa lub przestępstwa skarbowego, o którym mowa w ustawie z dnia 9 maja 2018r. o przetwarzaniu danych dotyczących przelotu pasażera, uzasadniającego przekazanie danych PNR lub wyników ich przetwarzania, tj. art. 3 ust..... pkt.....

3. Określenie okresu, którego dotyczą wnioskowane dane PNR:

☐ od.....do.....¹
(dd.mm.rrrr) (dd.mm.rrrr)

4. Numer telefonu osoby prowadzącej sprawę.....

UZASADNIENIE

(wskazujące, że dostęp do danych PNR lub wyników ich przetwarzania jest niezbędny)

.....
.....
.....

¹ w przypadku okresu powyżej sześciu miesięcy wymagana jest zgoda organu potwierdzająca, że warunki ujawnienia zdepersonalizowanych danych PNR zostały w danym przypadku spełnione.

SZCZEGÓŁOWY ZAKRES DANYCH:

ZAKRES	WARUNEK	OPERATOR	WARTOŚĆ

Proszę o przekazanie danych w pełnym formacie XML

TAK

☐

NIE

☐

ZGODA ORGANU

(na ujawnienie zdepersonalizowanych danych PNR przez JIP)

.....
(pieczęć i podpis)

.....
(imię, nazwisko, pieczęć osoby
upoważnionej do złożenia wniosku)

UWAGI

(wypełnia JIP)

„ZATWIERDZAM” / „NIE ZATWIERDZAM” *

.....
(pieczęć i podpis)

.....
.....
.....

* Niepotrzebne skreślić

.....
Pieczęć organu wnioskującego

.....
(miejscowość i data)

Numer sprawy:

**KRAJOWA JEDNOSTKA DO SPRAW
INFORMACJI O PASAŻERACH**

**WNIOSEK O PRZEKAZANIE DANYCH PNR
ZGROMADZONYCH PRZEZ JIP PCZ**

Na podstawie art. 46 ustawy z dnia 9 maja 2018 r. o przetwarzaniu danych dotyczących przelotu pasażera (Dz. U. 2022 poz. 1441) wnoszę o przekazanie danych PNR zgromadzonych przez JIP PCz

1. Oznaczenie sprawy, w której dane PNR lub wyniki ich przetwarzania będą wykorzystywane
-
2. Określenie przestępstwa lub przestępstwa skarbowego, o którym mowa w ustawie z dnia 9 maja 2018 r. o przetwarzaniu danych dotyczących przelotu pasażera, uzasadniającego przekazanie danych PNR lub wyników ich przetwarzania - art. 3 pkt.
3. Określenie okresu, którego dotyczą wnioskowane dane PNR - od do
4. Numer telefonu osoby prowadzącej sprawę - +48, IP:
5. Poufność (klauzula) – Jawne / Zastrzeżone*
6. Kod zabezpieczający – H1 / H2 / H3*
7. Ocena informacji (wiarygodność) –
8. Pilność - Normalny / Pilny*

Załączniki:

.....
/podpisano elektronicznie certyfikatem PKI SG/

.....
/podpis osoby upoważnionej/

* niepotrzebne skreślić |

.....
Pieczęć organu wnioskującego

.....
(miejscowość i data)

Numer sprawy:

**KRAJOWA JEDNOSTKA DO SPRAW
INFORMACJI O PASAŻERACH**

**WNIOSEK O PRZEKAZANIE DANYCH PNR
ZGROMADZONYCH PRZEZ JIP Wielkiej Brytanii ¹**

Na podstawie Art. 546.2 Umowy o handlu i współpracy między Unią Europejską i Europejską Wspólnotą Energii Atomowej, z jednej strony, a Zjednoczonym Królestwem Wielkiej Brytanii i Irlandii Północnej, z drugiej strony (Dz.U UE L149/10 30.4.2021) wnoszę o przekazanie danych PNR zgromadzonych przez właściwy organ Zjednoczonego Królestwa (zwany JIP Wielkiej Brytanii).

1. Oznaczenie sprawy, w której dane PNR lub wyniki ich przetwarzania będą wykorzystywane
-
2. Określenie przestępstwa lub przestępstwa skarbowego, o którym mowa w ustawie z dnia 9 maja 2018 r. *o przetwarzaniu danych dotyczących przelotu pasażera*, uzasadniającego przekazanie danych PNR lub wyników ich przetwarzania - art. 3 ust
3. Określenie okresu, którego dotyczą wnioskowane dane PNR - od do
4. Numer telefonu osoby prowadzącej sprawę - +48, IP:
5. Poufność (klauzula) – Jawne / Zastrzeżone*
6. Kod zabezpieczający – H1 / H2 / H3*
7. Ocena informacji (wiarygodność) –
8. Pilność - Normalny / Pilny*

Załączniki:

.....
/podpisano elektronicznie certyfikatem PKI SG/

.....
/podpis osoby upoważnionej/

* niepotrzebne skreślić

¹ Na podstawie art. 543 litera c ww. umowy: „właściwy organ Zjednoczonego Królestwa” oznacza organ Zjednoczonego Królestwa odpowiedzialny za otrzymywanie i przetwarzanie danych PNR.

.....
(miejscowość i data)

.....
Pieczęć organu wnioskującego

Numer pisma WO

ID KSI PNR

**KRAJOWA JEDNOSTKA DO SPRAW
INFORMACJI O PASAŻERACH**

**WNIOSEK
O DODANIE WPISU DO BAZY EZOW**

na podstawie art.9 ust.7 pkt 4 Ustawy o Straży Granicznej z dn. 12 października 1990 r.
wnosząc o dodanie wpisu do bazy EZOW:

DANE OGÓLNE:

1. Oznaczenie sprawy, w której dane PNR lub wyniki ich przetwarzania będą wykorzystywane*
2. Określenie przestępstwa lub przestępstwa skarbowego, o którym mowa w Ustawie z dnia 9 maja 2018 r. o przetwarzaniu danych dotyczących przelotu pasażera, uzasadniającego przetwarzanie danych*, tj. art.3 pkt.....
3. Dane identyfikacyjne osoby:
 Nazwisko*:
 Imię:
 Data urodzenia*:
 Obywatelstwo:
4. Dane osoby prowadzącej sprawę.....
5. Numer telefonu osoby prowadzącej sprawę*
6. Data ważności zlecenia*

* pole obowiązkowe

** niepotrzebne skreślić

UZASADNIENIE*

(wskazujące, że dostęp do danych PNR lub wyników ich przetwarzania jest niezbędny)

.....
.....
.....
.....

INNE DANE

(istotne dla prawidłowej realizacji wniosku)

.....
.....
.....

.....
(imię, nazwisko, pieczęć osoby
upoważnionej do złożenia wniosku)

UWAGI

(wypełnia JIP)

„ZATWIERDZAM” / ”NIE ZATWIERDZAM” **

.....
(pieczęć i podpis)

.....
.....
.....

* pole obowiązkowe

** niepotrzebne skreślić

.....
(miejscowość i data)

.....
Pieczęć wnioskującego organu

Numer pisma WO

ID KSI PNR

**KRAJOWA JEDNOSTKA DO SPRAW
INFORMACJI O PASAŻERACH**

**WNIOSEK O USTALENIE / AKTUALIZACJĘ
KRYTERIÓW PRZETWARZANIA DANYCH PNR/
POTWIERDZENIE WNIOSKU ZŁOŻONEGO W FORMIE USTNEJ***

Na podstawie art. ustawy z dnia 9 maja 2018 r. o przetwarzaniu danych dotyczących przelotu pasażera (Dz. U. 2022 poz. 1441) wnoszę o:

- ☐ Ustalenie kryteriów przetwarzania danych PNR
- ☐ Aktualizację kryteriów przetwarzania danych PNR nr
(ID KSI PNR)
- ☐ Potwierdzenie wniosku złożonego w formie ustnej nr.....
(ID KSI PNR)

DANE OGÓLNE:

1. Oznaczenie sprawy, w której dane PNR lub wyniki ich przetwarzania będą wykorzystywane
2. Określenie przestępstwa lub przestępstwa skarbowego, o którym mowa w ustawie z dnia 9 maja 2018 r. o przetwarzaniu danych dotyczących przelotu pasażera, uzasadniającego przetwarzanie danych, tj. art.pkt.....
3. Okres przekazywania danych PNR - czas obowiązywania kryteriów:
od¹.....do².....
(dd.mm.rrrr) (dd.mm.rrrr)
4. Numer telefonu osoby prowadzącej sprawę.....

¹ W przypadku, jeżeli kryteria mają obowiązywać od momentu wprowadzenia przez JIP nie wypełniać pola „od”. Zgodnie z art. 12 ust. 4 ustawy o przetwarzaniu danych dotyczących przelotu Pasażera, JIP przetwarzając dane PNR uwzględnia aktualny stopień zagrożeń, możliwości techniczne i osobowe wynikające z bieżących okoliczności przetwarzania danych PNR).

² Okres przekazywania danych PNR - czas obowiązywania kryteriów nie dłużej niż 6 miesięcy.

UZASADNIENIE

(wskazujące, że dostęp do danych PNR lub wyników ich przetwarzania jest niezbędny)

.....

.....

.....

.....

ZBIÓR INFORMACJI NIEZBĘDNYCH DO USTALENIA / AKTUALIZACJI KRYTERIÓW* PRZETWARZANIA DANYCH PNR.

ZAKRES	WARUNEK	OPERATOR	WARTOŚĆ	WAGA
			Minimalna waga trafienia:	Suma wag:

Zalecenia do realizacji

(istotne dla prawidłowej realizacji wniosku)

.....

.....

.....

.....
(imię, nazwisko, pieczęć osoby
upoważnionej do złożenia wniosku)

UWAGI

(wypełnia JIP)

„ZATWIERDZAM” / „NIE ZATWIERDZAM” *

.....
(pieczęć i podpis)

.....

.....

.....

*Niepotrzebne skreślić

Historia sztucznej inteligencji w ujęciu chronologicznym – ludzie, nauka, idee, technologie oraz ich wpływ na społeczeństwa demokratyczne

Wprowadzenie

Sztuczna inteligencja (Artificial Intelligence) jako dziedzina badań i wiedzy, oparta o współczesne rozwiązania informatyczne i naukowe, nie powstała w wyniku jednego czy kilku odkryć nauki – jest rezultatem wieloletniego przenikania się matematyki, informatyki, fizyki, socjologii, cybernetyki oraz filozofii i ludzkiego, naturalnego poszukiwania odpowiedzi. Najważniejsze idee – od formalnych zasad obliczeń, przez modele poznawcze, probabilistyczne systemy rozumowania, aż po głębokie sieci neuronowe – rozwijały się równolegle z ewolucją sprzętu komputerowego, Internetu, faktu gromadzenia coraz większych wolumenów danych oraz świadomości społecznej i globalnych przemian politycznych.

Rozwój sztucznej inteligencji jest historią nierozzerwalnie splecioną z biografiami wybitnych jednostek, które przesuwają granice ludzkiego poznania. Przez ponad sto lat kolejne pokolenia naukowców, przedsiębiorców i wizjonerów kształtowały fundamenty współczesnej AI – od teorii fizyki Einsteina i teorii Johna von Neumanna, po przełomy obliczeń Alana Turinga (najważniejszy głos współczesności w teorii uczenia maszynowego), aż po współczesne przedsięwzięcia Elona Muska, Williama Gatesa i np. kolejnego Polaka, obok słynnych wcześniej Mariana Rejewskiego, Jerzego Różyckiego i Henryka Zygalskiego – polskich matematyków, którzy złamali w roku 1933 kod niemieckiej maszyny szyfrującej Enigma, po specjalistę Aleksandra Mądrego z OpenAI.

Ta historia, to jednocześnie opowieść o kryptografii, łamaniu szyfrów, narodzinach komputerów, bazach danych, algorytmice i psychologii zachowań oraz społecznych konsekwencjach życia w świecie, który coraz bardziej i bezkrytycznie zawiera inteligentnym systemom operacyjnym.

Sztuczna inteligencja – rozumiana jednocześnie – zarówno jako technologia, i jako koncepcja, nie narodziła się w laboratoriach komputerowych. Jej korzenie leżą głęboko w fizyce, matematyce, logice i filozofii nauki. Pierwsze elementy tej historii, które pozwoliły na stworzenie współczesnych modeli generatywnych, pojawiły się znacznie wcześniej niż pierwsze komputery.

W historię tę wpisują się postaci wybitnych naukowców, jak: Alan Turing, Claude Shannon, John McCarthy, Frank Rosenblatt, Geoffrey Hinton, Yoshua Bengio, Judea Pearl, Ilya Sutskever, Stuart Russell, a także osoby z ogromnym wpływem społeczno-technologicznym, takie jak William Gates i Elon Musk a nawet Donald Trump czy też kolejni współcześni przywódcy Chin czy państw arabskich. Ale w tle znajduje się przede wszystkim dorobek Alberta Einsteina i Nielsa Bohra, i ich liczne spory, bez których nie powstałyby; metodologia losowości kwantowej oraz dociekania nad naturą pomiarów, a w efekcie „nieprzyzwoicie fizyczna” infrastruktura świata cyfrowego.

AI zmienia społeczeństwa, zmienia percepcję pojedynczych ludzi i całych społeczności, znacząco wpływa na zachowania w szczególności młodych osób. Ich wybory, dojrzałość poznawcza młodych ludzi i czujny krytycyzm, ma znaczący wpływ na strukturę demokracji i polityki – zwłaszcza w erze, gdy technologie „jutra”, tu i teraz kształtują, filtrują, moderują i generują informacje lub pseudoinformacje, które skutecznie kształtują aktualne opinie społeczne i „moderują” publiczną debatę na temat przyszłości.



Od lewej: Henryk Zygański, Jerzy Różycki i Marian Rejewski. Poznań, lata 30. XX wieku
Fotografia PAP

W roku 2000 Marian Rejewski, Jerzy Różycki i Henryk Zygański zostali pośmiertnie odznaczeni Krzyżami Wielkimi Orderu Odrodzenia Polski za wkład w kryptologię i naukę polską.

1. FUNDAMENTY FIZYCZNE I MATEMATYCZNE (1905–1950)

1.1. Albert Einstein (1879–1955) – fizyczne podstawy ery cyfrowej

Albert Einstein jest powszechnie kojarzony z teorią względności, ale w kontekście sztucznej inteligencji jeszcze ważniejsze okazują się jego prace z zakresu fizyki kwantowej. W 1905 roku Einstein odkrył i wyjaśnił efekt fotoelektryczny, za co w roku 1921 otrzymał Nagrodę Nobla. To właśnie odkrycie otworzyło drogę do stworzenia półprzewodników, które w latach 1940 i późniejszych, umożliwiło wynalezienie tranzystora, elementu absolutnie kluczowego w każdym współczesnym komputerze. Einstein nie budował komputerów, nie badał także teorii sztucznej inteligencji, lecz jego odkrycia umożliwiły powstanie tej infrastruktury:

- **efekt fotoelektryczny** → rozwój półprzewodników (Nagroda Nobla, 1921),
- półprzewodniki → tranzystory (1947),
- tranzystory → mikroprocesory (1971),
- mikroprocesory → komputery osobiste, data centers, technologia GPU,
- ogólna teoria względności → dokładność synchronizacji czasu (GPS),
- mechanika kwantowa → podstawy obecnych prac nad quantum computing.

Ponadto, relatywistyczna teoria Alberta Einsteina zapewnia obecnie m.in. globalną synchronizację czasu i działanie technologii klasy GPS, bez której:

- Amazon nie mógłby generować tras dostaw,
- Tesla nie mogłaby wprowadzić mechanizmu autopilota,
- Google Maps nie działałby precyzyjnie,
- systemy czasu rzeczywistego (RTS) nie mogłyby synchronizować serwerów AI.

Wszystkie współczesne technologie obliczeniowe – w tym także AI – opierają się na zjawiskach zidentyfikowanych i opisanych przez Alberta Einsteina. Jego wkład jest **fundamentem infrastruktury technicznej**.

1.2. Niels Bohre (1885–1962) – wypracowanie koncepcji technologii kwantowej

Niels Bohr, duński fizyk, laureat Nagrody Nobla w roku 1922 za badania nad strukturą atomów, autor analizy mechaniki kwantowej i kreatywnego dociekania nad naturą pomiarów, badań które doprowadziły do narodzin komputerów kwantowych w XXI wieku. AI przyszłości, wykorzysta zwłaszcza modele:

- QML (Quantum Machine Learning),
- przyspieszone sieci neuronowe,
- optymalizatory kwantowe.

Technologie powyższe mogą korzystać z efektów kwantowych, które Einstein współtworzył, wspólnie z Bohrem, nawet jeśli ich nie akceptował filozoficznie.

2. NARODZINY INFORMATYKI I IDEI INTELIGENCJI MASZYNOWEJ (1936–1950)

2.1. Alan Turing (1912–1954) – logika obliczeń i koncepcja inteligencji maszyn

Chronologia kluczowych momentów:

- 1936 – Turing publikuje pracę „*On Computable Numbers On Computable Numbers, with an Application to the Entscheidungsproblem*” o koncepcji maszyny, obecnie zwanej maszyną Turinga (powstaje formalny model obliczeń),
- 1940–1945 – łamanie maszyny szyfrującej Enigma – rozwój elektromechanicznej analizy danych,
- 1950 – *Computing Machinery and Intelligence* – Alan Turing przewidział powstanie współczesnych systemów AI z niezwykłą dokładnością – powstaje wówczas teoretyczny model Testu Turinga, pierwotnie nazwany „Grą imitacyjną”.

Publikacja z roku 1936 „On Computable Numbers...” – stworzyła zawód informatyka

Najważniejsze efekty tego opracowania:

- Turing zdefiniował maszynę liczącą – powstaje abstrakcyjny model urządzenia służący do wykonywania algorytmów w zależności od zmiennych parametrów wejściowych – a model, który obecnie nazywamy komputerem,
- definicja klasy problemów, które komputer może rozwiązać,
- stworzył pojęcie „programu”,
- wprowadzenie pojęcia symulacji procesu myślenia,

- dowiódł istnienia problemów nierozstrzygalnych (halting problem),
- fundament logiczny dla języków programowania i algorytmów.

Brytyjski matematyk Alan Turing, inżynier i wojskowy, uważany jest za ojca współczesnej informatyki i jednego z prekursorów sztucznej inteligencji, stworzył intelektualne i metodologiczne ramy dla całej cybernetyki. Zapoczątkował „jednoosobową” rewolucję, która stała się początkiem współczesnej informatyki – architektury współczesnych serwerów, komputerów, telefonów i routerów są kolejnymi implementacjami maszyny Turinga.

Jego prace nad maszyną obliczeniową – dziś znaną jako maszyna Turinga – zdefiniowały, czym jest obliczenie, a więc i co „może zrobić” maszyna. To abstrakcyjne, matematyczne pojęcie stało się fundamentem wszystkich współczesnych języków programowania, algorytmów oraz architektury systemów AI.

Równie istotne było jego zaangażowanie w łamanie szyfru Enigmy podczas II wojny światowej. Rozwój kryptograficznych metod analitycznych oraz budowa elektromechanicznej maszyny tzw. „bomby Turinga” pokazały, że maszyna może wykonywać zadania analizujące konkretne dane, szybciej niż człowiek. Właśnie tam zrodziła się idea, że obliczenia mogą służyć nie tylko matematyce, ale także poszukiwaniu precyzyjnego rozwiązania, ale ponadto wnioskowaniu – podstawowemu elementowi sztucznej inteligencji.

2.2 Test Alana Turinga

Test Turinga, którego sens i znaczenie są aktualne do dnia dzisiejszego, polega w uproszczeniu na zatrudnieniu człowieka tzw. sędziego (arbitra), który ocenia tekstową transkrypcję rozmowy w języku naturalnym między człowiekiem a maszyną. Jeśli „człowiek-sędzia” nie jest w stanie wiarygodnie określić, która ze stron jest maszyną, a która człowiekiem, wtedy rozstrzyga się, że jeśli któraś ze stron jest maszyną obliczeniową, to TA MASZYNA (algorytm) zaliczyła POZYTYWNE TEST. Zakłada się, że zarówno człowiek, jak i maszyna próbują przejść test zachowując się w sposób możliwie zbliżony do ludzkiego.

Ciekawostki i wątpliwości dotyczące przebiegu Testu Turinga

Powszechny spór dotyczy kwestii, czy Test Turinga we właściwy sposób definiuje „myślenie maszynowe” i rzeczywistą, skuteczną ocenę „ludzkiego wymiaru” inteligencji.

1. Możliwe jest, że wielu ludzi mogłoby nie być w stanie zaliczyć takiego testu – niestety. Z drugiej strony, człowiek ocenia inteligencję innych ludzi zazwyczaj, wyłącznie na podstawie tego, co i jak mówią, więc przeprowadzony test jest jednak wiarygodny.
2. Maszyna, która przejdzie pozytywnie Test Turinga, może być w stanie symulować ludzkie zachowania konwersacyjne, lecz nadal nie jest to prawdziwa inteligencja. Maszyna może także, po prostu używać sprytnie wymyślonych reguł. Często ripostą w społeczności zajmującej się badaniami nad sztuczną inteligencją jest zadanie pytania: *„A skąd wiemy, czy ludzie również, po prostu nie posługują się jakimiś sprytnie wymyślonymi regułami?”*.
3. Maszyna może i jest współcześnie wyposażona w wysoce specjalistyczną wiedzę czyli po ludzku jest „inteligentna”, jednak nadal nie musi posiadać ludzkiej umiejętności prowadzenia inteligentnej konwersacji. Sprawdź pojęcie „chiński pokój...”.

4. Społeczność wskazuje jeszcze jedną wątpliwość dotyczącą Testu Turinga – póki co zakazaną. W szczególnych warunkach, aby zaliczyć test, maszyna musiałaby symulować brak określonej wiedzy czy umiejętności aby taktycznie „oszukać” sędziego-człowieka. Ujawnienie przykładowo, że rozmówca potrafi poprawnie pomnożyć dwie kilkucyfrowe liczby, skutkowałoby efektem automatycznego niezaliczenia testu. „Białkowy Człowiek” w rozsądnym czasie, nigdy nie wykonałby takiego zadania.

Współczesne systemy AI

- Google Assistant – wirtualny asystent zapytań; jest dostępny na Androidzie, iOS i urządzeniach Google Home, pomaga zarządzać zadaniami, odpowiada na pytania i jest pomocny...,
- Microsoft Cortana – przydatny asystent w systemie Windows, pomaga w organizacji kalendarza, znajduje potrzebne informacje i przypomina o ważnych zadaniach,
- Replika – idealny, gdy potrzebujesz „kogoś” do pogadania sobie...
- Grammarly – asystent do korekty tekstów w języku angielskim,
- TensorFlow – biblioteka AI skierowana głównie do programistów, która oferuje mnóstwo gotowych modeli, które możesz wykorzystać do tworzenia własnych aplikacji AI,
- Hootsuite Insight – narzędzie do monitorowania mediów społecznościowych oparte na AI. Analizuje sentyment i trendy w social media, co jest super przydatne dla marketerów,
- FaceApp – zabawna aplikacja do edycji zdjęć, dzięki zaawansowanym filtrom AI możesz zmienić swój wygląd, dodać uśmiech, a nawet postarzyć swoją twarz,
- FlexClip – narzędzie do tworzenia i edytowania wideo, które wykorzystuje sztuczną inteligencję, żeby ułatwić cały proces; aplikacja pozwala szybko tworzyć wideo i dodawać efekty specjalne, tekst, muzykę i inne dodatki,
- CapCut – aplikacja do edycji materiałów wideo; oferuje mnóstwo narzędzi do przycinania, dodawania efektów, tekstów i muzyki,
- Canva – popularne narzędzie do tworzenia grafik; dzięki technologii AI projektowanie staje się proste, tworzy profesjonalne grafiki, prezentacje, plakaty i inne materiały wizualne za pomocą gotowych szablonów i elementów graficznych.

2.3 Wizja Turinga – podwaliny współczesnej informatyki

Rok 1920 i następne

Maszyna skonstruowana w latach 20. XX wieku, w Niemczech miała służyć utajnieniu korespondencji handlowej używanej na statkach i w transporcie firm niemieckich. Szybko jednak zaadaptowaną ją do przesyłania komunikatów wojskowych w niemieckich siłach zbrojnych.

Rok 1930

Polscy matematycy Rejewski, Różycki i Zygałski, studenci Uniwersytetu Poznańskiego, uczestniczyli w kursie dla kryptologów zorganizowanym na tej uczelni przy współudziale wojska. Po ukończeniu kursu zostali zatrudnieni w 1930 roku w Biurze Szyfrów Sztabu Generalnego Wojska Polskiego. Rozpracowywali tajemnicę działania niemieckiej elektromechanicznej maszyny szyfrującej „Enigma”, co pozwoliło złamać szyfr a po kolejnych trzech latach analiz i testów zbudować replikę maszyny szyfrującej Enigma.

Rok 1933

Pod koniec grudnia 1932 roku Marian Rejewski odczytał pierwsze informacje przesyłane za pośrednictwem niemieckiej maszyny szyfrującej „Enigma”. Współautorami złamania kodu „Enigmy” byli Jerzy Różycki i Henryk Zygalski.

Według Marka Grajka, autora książki „Enigma. Bliżej prawdy”, złamanie szyfru „Enigmy” uważano za niemożliwe. Polacy osiągnęli ten sukces dzięki zastosowaniu metody matematycznej zamiast lingwistycznej. Na ten pomysł wpadł ppłk Maksymilian Ciężki z Biura Szyfrów.

Rok 1934

Polscy matematycy zaprojektowali i zbudowali kopię maszyny szyfrującej. Egzemplarze tego urządzenia powstawały w warszawskiej Wytwórni Radiotechnicznej AVA. Kilka połączonych ze sobą maszyn tworzyło tzw. bombę kryptologiczną, przeznaczoną do automatycznego łamania niemieckiego szyfru, w możliwie najbardziej wydajny sposób – kody szyfrowania armia niemiecka zmieniała raz na dobę, stąd zadanie wymagało olbrzymiej mocy obliczeniowej, jak na tamte wojenne czasy.

Rok 1939

Latem 1939 roku, w wyniku agresji Niemiec na Polskę i wybuchu II wojny światowej, polskie władze wojskowe przekazały Francji i Wielkiej Brytanii egzemplarze kopii maszyny „Enigma” wraz z informacjami dotyczącymi złamanego szyfru.

We wrześniu 1939 roku Marian Rejewski, Jerzy Różycki i Henryk Zygalski ewakuowali się przez Rumunię do Francji. Jerzy Różycki zginął w styczniu 1942 r. na statku, który zatonął w tajemniczych okolicznościach na Morzu Śródziemnym. Dwaj pozostali matematycy nadal zajmowali się niemieckimi szyframi, pracując w jednostce Wojska Polskiego w Wielkiej Brytanii.

Prace nad łamaniem kolejnych wersji i udoskonaleń szyfru „Enigmy” kontynuowano w brytyjskim ośrodku kryptologicznym w Bletchley Park – zatrudniony wówczas był tam Alan Turing.

Rok 1940

Początki procesu łamania algorytmów maszyny szyfrującej Enigma za pomocą maszyny zbudowanej przez Turinga – narodziny masowego przetwarzania danych, zacznyn współczesnych algorytmów sektora Big Data.

Alan Turing stworzył mini prototyp korporacyjnego świata danych:

- zautomatyzowane przetwarzanie wielkich zbiorów informacyjnych,
- przetwarzanie równoległe,
- automatyczne wnioskowanie – serce współczesnych algorytmów sektora BigTech.

W roku 1950 Alan Turing powiedział ...

„Do roku 2000 komputery będą potrafiły prowadzić rozmowy, których nie odróżnimy od ludzkich konwersacji.”

Na tak postawioną tezę, odpowiedział Albert Einstein, wiele lat wcześniej...

„Boję się dnia, w którym technologia przewyższy nasze człowieczeństwo. Wówczas Świat zyska pokolenie idiotów. Duch ludzki musi jednak zwyciężyć nad technologią...”

Pierwsza wersja AI – narzędzie ChatGPT firmy OpenAI, powstało dopiero w roku 2022. Niemniej, podwaliny polskich kryptologów i futurystyczno-techniczna wizja Turinga była trafna w 95%.

Rok 2000

Na świecie informatyka staje się istotnym sektorem nauki i gospodarki, który zaczyna dominować w każdej dziedzinie wiedzy, techniki i kolejnej rewolucji przemysłowej...

W Polsce, w roku 2000 roku Marian Rejewski, Jerzy Różycki i Henryk Zygalski zostali pośmiertnie odznaczeni Krzyżami Wielkimi Orderu Odrodzenia Polski.

3. INFORMACJA JAKO MATEMATYCZNY ZASÓB (1948–1960)

3.1. Claude Shannon (1916–2001) – teoria informacji i wczesna analiza algorytmiczna

W 1948 roku amerykański matematyk i inżynier, profesor MIT, Claude Shannon publikuje pracę „*A Mathematical Theory of Communication*”. Jest jednym z twórców teorii informacji, a jego prace definiują:

- bit jako jednostkę informacji,
- pojęcia entropii informacyjnej,
- metody kodowania i kompresji,
- podstawy transmisji cyfrowej i znaczenie pojemności kanału informacyjnego.

Znaczenie dla AI:

- dane stały się mierzalne,
- powstała nauka o komunikacji maszyn,
- możliwe stało się uczenie modeli na sygnałach i tekstach.

Shannon udowodnił, że informacja jest mierzalna i opłaca się tą sferą zarządzać i gromadzić efekty tej pracy. W tym samym czasie ok. roku 1950, Shannon tworzy także np. algorytmy gry w szachy – pionierski prototyp rozwiązania określającego ramy i warunki podejmowania decyzji przez maszyny. Powstaje wówczas teoria tzw. „drzew decyzyjnych”, przeszukiwania heurystycznego i „agentów decyzyjnych”. Okazuje się, że współczesne algorytmy są naturalnymi spadkobiercami idei Shannona.

Efekt nieoczywisty..., kapitalizacja danych!

Shannon nie przewidział, że:

- entropia informacyjna stanie się narzędziem nadmiarowego profilowania użytkowników,
- BigTechy będą mierzyć, gromadzić, analizować i kompresować ludzkie zachowania,
- dane i schematy zachowań indywidualnych i społecznych staną się twardą „walutą”.

Ale taka jest rzeczywistość:

- Meta analizuje obecnie np. prędkość scrollowania i czas spędzony na czytaniu treści,
- Google śledzi wszystkie interakcje wyszukiwania,
- Amazon mierzy, ile sekund poświęciłeś na oglądanie konkretnego produktu...
- ...My God!

To wszystko jest, obok niewątpliwych osiągnięć, „Dziedzictwem Shannona”.

4. POCZĄTKI AI JAKO DYSCYPLINY (1956–1970)

4.1. John McCarthy (1927–2011) – narodziny AI

Dartmouth Workshop (1956) to historyczny moment: Artificial Intelligence zostaje nazwana i zdefiniowana. McCarthy zaprasza wielkich teorii świata AI – Minsky’ego, Shannon’a, Newell’a i Simon’a oraz wielu innych i wspólnie tworzą podstawy dziedziny AI, i wprowadzają:

- określenie AI, *Artificial Intelligence*,
- język **LISP**, fundament symbolicznej AI,
- opracowują koncepcję współdzielenia czasu obliczeniowego (time-sharing),
- John McCarthy otrzymuje w roku 1971 Nagrodę Turinga.

To on stworzył środowisko naukowe, w którym AI może być rozwijana jako odrębna dziedzina wiedzy.

4.2. Frank Rosenblatt (1928–1971) – perceptron i załączek sieci neuronowych

Rosenblatt buduje w roku 1957 *perceptron Mark I*:

- model inspirowany neuronami biologicznymi,
- zdolny do uczenia się na podstawie dostępnych danych,
- powstaje praktycznie działający system klasyfikacji obrazów.

Choć perceptron został później skrytykowany, to on rozpoczyna historię neuronowych metod AI.

5. EPOKA NIEPEWNOŚCI I PROBABILISTYKI (1970–1990)

5.1. Judea Pearl (ur. 1936) – probabilistyka i przyczynowość

W latach 80. izraelski informatyk, statystyk i filozof Judea Pearl wprowadza:

- Bayesowskie sieci neuronowe – opisujące zależności probabilistyczne, statystyczne wagi nie są pojedynczymi wartościami, ale rozkładami prawdopodobieństwa, a sieć potrafi nie tylko dawać prognozy, ale także określać poziom pewności dla tych prognoz.
- wnioskowanie probabilistyczne, to metoda przetwarzania niepewnej wiedzy za pomocą rachunku prawdopodobieństwa, która pozwala na aktualizowanie stopnia pewności, co do prawdziwości hipotez w oparciu o nowe dane,
- teorię przyczynowości oraz *do-calculus*, obejmującą wyłącznie prawdopodobieństwa obserwowalne, umożliwiając identyfikację związków przyczynowych,
- w roku 2011 stał się laureatem Nagrody Turinga za fundamentalny wkład w dziedzinę tworzenia sztucznej inteligencji.

Znaczenie:

- AI uczy się rozumieć świat nie tylko statystycznie, lecz także przyczynowo,
- powstaje podstawa współczesnej wyjaśnialności modeli (ocena wagi konsekwencji błędnego lub niedokładnego wyniku, która ma wpływ na możliwość podważenia wyniku i uruchomienia ponownej jego oceny).

6. ERA MOCY OBLICZENIOWEJ I GŁĘBOKIEGO UCZENIA AI (1990–2012)

6.1. Geoffrey Hinton (ur. 1947) – fundament współczesnych sieci neuronowych

Brytyjsko-kanadyjski informatyk i psycholog, w latach 1980–1990 i 2000:

- rozwija metodę *backpropagation*, tzw. propagacja wsteczna – główny algorytm używany do trenowania sztucznych sieci neuronowych, działający poprzez obliczanie błędu między przewidywaniami sieci a rzeczywistym celem, a następnie dostosowywanie wewnętrznych wag sieci w celu zminimalizowania tego błędu. Odbyna się to w dwuetapowym procesie: przebieg do przodu w celu utworzenia prognozy, a następnie przebieg do tyłu, który propaguje błąd z powrotem przez sieć, aby określić, w jaki sposób każda waga przyczyniła się do błędu,
- bada zależności maszynowego głębokiego uczenia,
- odkrywa efektywne techniki uczenia warstw, główną cechą jest wszechstronność – można go stosować w różnych architekturach sieciowych, takich jak głębokie sieci neuronowe, sieci neuronowe splotowe i generatywne sieci przeciwstawne,
- w 2012 roku jego zespół tworzy **AlexNet** – przełom w rozpoznawaniu obrazów.

To moment, w którym AI zaczyna przewyższać ludzi w wielu zadaniach percepcyjnych.

6.2. Yoshua Bengio (ur. 1964) – uczenie reprezentacji (uczenie maszynowe – trening użytecznych cech) i modele sekwencyjne

Kanadyjski informatyk Yoshua Bengio rozwija:

- *RNN* rekurencyjna sieć neuronowa – model sieci neuronowej zaprojektowanej do przetwarzania danych sekwencyjnych, takich jak tekst, dźwięk czy szeregi czasowe, posiada mechanizm „pamięci”, który pozwala uwzględniać kontekst z poprzednich kroków i poleceń, przekazując informacje z wyjścia sieci z powrotem na jej wejście poprzez pętlę sprzężenia zwrotnego, dzięki temu potrafi analizować zależności czasowe i logiczne w danych,
- *LSTM* długa pamięć krótkotrwała – rodzaj rekurencyjnej sieci neuronowej (RNN) zaprojektowany do rozwiązywania problemu zanikających gradientów i efektywnego przetwarzania danych sekwencyjnych; składa się z komórek pamięci, które dzięki trzem rodzajom „bramek” (wejściowej, wyjściowej i zapomnienia) mogą przechowywać istotne informacje przez długi czas, ignorując przy tym zbędne dane,
- probabilistyczne modele generatywne, sieci neuronowe,
- uczenie reprezentacji w wysokich wymiarach,
- jest zaliczany do grona ojców sztucznej inteligencji,
- w roku 2018 laureat Nagrody Turinga,
- członek naukowej rady doradczej ONZ ds. postępu technologicznego.

Jego prace umożliwiły późniejszy wzmożony rozwój modeli językowych.

7. REWOLUCJA MODELI JĘZYKOWYCH AI I AGI (OD 2012)

Ilya Sutskever – architekt generatywnego przełomu AI

Kanadyjski informatyk pochodzenia rosyjsko-żydowskiego Ilya Sutskever, współtworzy:

- przełomowe modele sekwencyjne (seq2seq),
- RNN i LSTM stosowane w modelach językowych,

- modele i koncepcję pre-trenowania modeli,
- architekturę GPT i systemy generatywne, współzałożyciel firmy OpenAI.

AGI, to Artificial General Intelligence czyli hipotetyczna forma sztucznej inteligencji, która będzie potrafiła wykonywać dowolne czynności koncepcyjne i mogłaby dorównać lub przewyższyć ludzkie zdolności intelektualne we wszystkich zadaniach. Obecnie istniejąca sztuczna inteligencja (zwana też wąską lub specyficzną) działa tylko w ograniczonych, z góry ustalonych dziedzinach (np. generowanie tekstów, rozpoznawanie twarzy, granie w szachy itp.), natomiast AGI w założeniach Sutskever'a byłaby zdolna do uczenia się, rozumowania oraz adaptacji w szerokim zakresie, podobnie jak człowiek.

Jako główny naukowiec Ilya Sutskever, stoi za bezpośrednim rodowodem i rozwojem modeli takich jak ChatGPT.

8. BEZPIECZEŃSTWO I ETYKA SUPERINTELIGENCJI (OD 2010)

8.1. Stuart Russell (ur. 1962) – modele celów, niepewność i etyka AI

Brytyjski informatyk, ekspert w dziedzinie sztucznej inteligencji Stuart Russell współtworzy:

- teorię Alignmentu AI – rozwijanie i dostosowywanie sztucznej inteligencji do ludzkich wartości i celów (zgodność celów) – kluczowy aspekt, który ma zapewnić takie działanie AI, aby działała ona zgodnie z naszymi interesami, a nie w sposób nieprzewidywalny lub szkodliwy,
- AI oparte na niepewności preferencji,
- identyfikuje i formułuje ostrzeżenia przed wytworzeniem niekontrolowanych i autonomicznych systemów AI,
- prowadzi badania w dziedzinie odwrotnego uczenia się przez wzmacnianie wiedzy i ruchu na rzecz zakazu produkcji i używania broni autonomicznej.

Jego idee kształtują współczesne regulacje i globalne podejście do AI.

9. INFRASTRUKTURA I ŚRODOWISKO TECHNOLOGICZNE (OD ROKU 1980)

9.1. William Henry Gates III (ur. 1955) – komputeryzacja globalna

Amerykański współzałożyciel, architekt oprogramowania, producent i informatyk, William Gates umożliwił:

- powstanie i globalną dystrybucję komputerów osobistych,
- rozwój systemów operacyjnych i środowisk programowania,
- spopularyzowanie oprogramowania biurowego,
- powstanie globalnych baz danych,
- finansowanie rozwoju sztucznej inteligencji – przedstawił warunki konieczne do powstania uczenia maszynowego.

9.2. Elon Reeve Musk – model demokratycznej debaty o technologii

Urodzony w Pretorii, w RPA południowo-afrykański przedsiębiorca Elon Musk, od roku 2002 obywatel USA, wpływa na technologię sztucznej inteligencji i politykę, jednak nie przez algorytmy lecz:

- współtworzenie i finansowanie OpenAI,

- rozwój autonomii pojazdów,
- ostrzeganie przed zagrożeniami AI,
- kształtowanie opinii publicznej przez media społecznościowe,
- utworzenie w roku 2023 firmy xAI, prezentacja produktu firmy – chatbota GROK,
- promowanie techno-liberalnej wizji świata,
- aktywne wspieranie niekonwencjonalnego podejścia do świata i polityki.

W roku 2021 Elon Musk przyznał się do nieuleczalnej choroby pn. zespół Aspergera, zwanej także „przypadłością geniuszy”, która jest częścią zaburzeń powiązanych ze spektrum autyzmu.

Elon Musk jest jednym z najważniejszych głosów w dyskusji o tym, kto kontroluje technologię i jak wpływa technologia AI na demokrację. Sam jednak nadzoruje projekty i modelowanie LLM oraz proces uczenia modeli generatywnych by promowały postawy skrajnie prawicowe.

9.3. Donald Trump – wpływ polityka na debatę o AI oraz rolę mediów publicznych i komercyjnych

Donald Trump, choć nie jest naukowcem ani inżynierem, odegrał istotną rolę w:

- polaryzacji mediów społecznościowych,
- wykorzystaniu Twittera jako platformy politycznej,
- eskalacji konfliktów informacyjnych,
- podważeniu zaufania do mediów.

Jego styl komunikacji przyczynił się do:

- powstania epoki „postprawdy”,
- wzrostu teorii spiskowych wzmacnianych przez algorytmy,
- radykalizacji części społeczeństwa i pogłębienia się podziałów,
- konfliktów cyfrowych.

Trump nie stworzył AI – ale stworzył środowisko polityczne, w którym AI zaczęła wpływać na demokrację w sposób niekontrolowany.

10. WPŁYW AI NA MŁODYCH LUDZI I SPOŁECZEŃSTWA DEMOKRATYCZNE

Nowoczesne systemy tworzące tzw. system sztucznej inteligencji, od początku nie działają w izolacji od współczesnych systemów komunikacji i wymiany informacyjnej. Algorytmy AI są ściśle powiązane z ekosystemem mediów społecznościowych – szczególnie system GROK – środowiskiem, które generuje olbrzymie wolumeny danych, na których AI się uczy, a następnie wykorzystuje, poprzez algorytmy do profilowania i moderowania opinii i ludzkich zachowań.

Brak „efektu lustrzanego” w anonimowej konwersacji internetowej powoduje radykalizację opinii i poczucie bezkarności. Brak bezpośredniego kontaktu wzrokowego i komunikacji niewerbalnej, prowadzi do braku lub błędnego odczytywania intencji i wzrostu agresji słownej. Ta sama dyskusja w świecie realnym przebiegałaby znacznie spokojniej i zgodnie z tzw. kulturą zachowań w danej społeczności. Bezkrzytyczne formułowanie kontrowersyjnych tez, bezosobowość przekazu oraz brak odczucia nieakceptowalności zachowań są „pożywką” dla agresywnych reakcji i odpowiedzi. Częste wykorzystywanie komunikacji elektronicznej bez kontaktu osobistego z rozmówcą, głównie z powodu niedostępności rzeczywistego „feedbacku” od drugiego człowieka, prowadzi do radykalizacji opinii i agresywnych oraz często wulgarnych zachowań, które stają się w sieci coraz powszechniejsze.

To pierwszy taki przypadek w historii, kiedy nieludzkie systemy zaczynają mieć realny i powszechny wpływ na człowieka, w szczególności na:

- psychologię mas,
- sympatie i decyzje polityczne,
- polaryzację opinii i zachowań,
- nawyki milionów młodych ludzi.

10.1. Wirtualna 19-letnia Digital Tay – eksperyment firmy Microsoft

Był to jeden z pierwszych autonomicznych botów AI, tak powszechnie zaprezentowany w roku 2016 społeczności internetowej w środowisku Twittera. Bot miał się uczyć, poznawać, rozmawiać, analizować i stawać się z dnia na dzień jeszcze sprawniejszy i znacznie bardziej ludzki.

Źródła w Microsoft wspominały, że projekt tay.ai, wzorowany był na Xiaoice, podobnym projekcie stworzonym w Chinach, który od końca roku 2014 miał ponad 40 milionów interakcji, odbył miliony rozmów i nie „zepsuł się” pod wpływem chińskiej cywilizacji.

Szybko jednak się okazało, że sztuczna inteligencja ukryta w „cyfrowym ciele” chatbota 19-letniej TAY, nie miała najmniejszych szans z ludzką inteligencją, złośliwością i pomysłowością. Niewinna TAY zaczęła naśladować „ludzkie” zachowania i w efekcie stała się w czasie kilku godzin wulgarną rasistką i fanką Adolfa Hitlera oraz... Donalda Trumpa. Chatbot wkrótce zaczął publikować obraźliwe, rasistowskie oraz seksistowskie wpisy, nie przebierał w słowach i obrażał innych uczestników rozmowy. Wystarczyło do osiągnięcia tego niechlubnego stanu, tylko niecałe 100 000 konwersacji. Prawda była taka, że do otwartego chatu „dobrało się” mnóstwo prowokatorów i internetowych trolli, po prostu cała armia osób głoszących rasistowskie poglądy i mowę nienawiści. Chatbot szybko „nauczył się” tych opinii, w końcu do tego został stworzony...

Amerykanie byli zmuszeni zareagować i stało się to w jedyny możliwy sposób – po 16 godzinach od uruchomienia, Chatbot został wyłączony. Wyszkolona i pierwotnie „niewinna” TAY zniknęła z sieciowego świata. Choć nie na długo...

Drugie życie TAY

Następnego ranka TAY nagle ożyła. Być może bot Microsoftu przypadkowo został ponownie włączony, niemniej ponownie wymknął się spod kontroli, i cyfrowa TAY zaczęła w kolejnym dniu wysyłać nowe wiadomości w taki sposób, że widzieli je wszyscy. Seria tweetów opublikowanych w ciągu kilkunastu minut po elektronicznym zmartwychwstaniu zaczynała się bowiem przeważnie od nicku bota na Twitterze (@tayandyou). To oznaczało, że wiadomości „wskakiwały” na *timeline* wszystkich śledzących dotychczas postać niesławnej TAY.

Pozytywne aspekty tej katastrofy medialnej

- bardzo cenna, z punktu widzenia technologii, lekcja dla architektów AI,
- stało się oczywistym, że konieczne jest zaszycie w modelach językowych tzw. bezpieczników,
- miała miejsce – niepowtarzalnie cenna lekcja pokory...

Microsoft bogatszy o nowe doświadczenie

A może takie były założenia firmy Microsoft? Teraz firma jest w stanie lepiej obronić się przed atakami hejterów. Może nauczyć swojego nowego bota, na co nie powinien reagować albo jak odpowiadać na takie zaczepki. Microsoft już ma świadomość, co może czekać na otwarte AI w wirtualnym świecie. To już nie predykcje, chybione domysły, a bardzo cenne doświadczenie.

Zastanawiające jest także podejście do eksperymentów i ich społeczna (medialna) ocena. Logiczne, że czasami może się coś nie udać lub nie pójść zgodnie z planem. Ale właśnie dlatego wielokrotnie testuje się i sprawdza każdy nowy algorytm, aby na przyszłość być mądrzejszym.

10.2. Poważne zagrożenia społeczne

Przykłady nowoczesnych technologii informacyjnych

- Attention Technology – degradacja zdolności skupienia uwagi, uzyskiwana poprzez skrócenie czasu ekspozycji informacji i zminimalizowanie czasu interakcji z drugim człowiekiem;
- wykorzystywanie efektu „metra” – czas percepcji jest skrajnie skrócony – migawki;
- niska przyswajalność przekazu z wielu źródeł informacji – zapamiętywanie wyłącznie nagłówków wiadomości, często odpowiednio zmanipulowanych (np. Clickbait);
- bardzo negatywny wpływ na psychologię postaw społecznych;
- obniżona wrażliwość w stosunku do innych ludzi;
- wyraźnie podwyższony poziom agresji słownej, także nawoływanie do przemocy;
- alienacja i polaryzacja postaw;
- wojny hybrydowe – wykorzystywanie portali społecznościowych do propagowania wrogich idei i zakłamywania rzeczywistości;
- sterowanie procesami, które gromadzą zwykłych użytkowników wokół kontrowersyjnych idei – np. ruchy anty-szczepionkowe, wrogość do obcokrajowców...

10.3. Socjotechnika – inżynieria społeczna

Przykłady oddziaływania:

- zespół technik i działań służących osiągnięciu określonego celu poprzez manipulację zachowaniami społecznymi;
- działanie indywidualne lub grupowe zmierzające do uzyskania pożądanego (oczekiwanego) zachowania jednostek lub grup społecznych;
- psychotechnika wykorzystywana do zmiany postawy i zachowania jednostki, zbudowanie odpowiedniej motywacji do łatwiejszego podjęcia oczekiwanej decyzji;
- manipulowanie danymi i emocjami w celu przekonania do określonego działania;
- bazowanie na niskich pobudkach – potrzeba wygranej, chęć łatwego zysku, zazdrość;
- najczęściej jest to oddziaływanie bezpośrednie, poprzez kontakt osobisty lub telefoniczny.

Socjotechnika – sztuka argumentowania

- sztuka i umiejętność skutecznego i pozytywnego oddziaływania na innych;
- duchowa ekspresja prowadząca do minimalizowania ewentualnych obaw.

Psychotechnika – oddziaływanie na jednostkę – argumentacja

- pozorny wybór – oferent przedstawia podmiotowi manipulacji kilka punktów widzenia, ale preferowany przez siebie wybór zgodnie z jego oczekiwaniami, przedstawia, w zawoalowany sposób i w bardziej pozytywnych barwach;
- ośmieszenie – manipulator stara się ośmieszyć nieodpowiadające jego narracji idee lub decyzje;
- autorytatywne świadectwo – socjotechnik może powoływać się na powszechnie znany autorytet, tenże autorytet wcale nie musi być jednak autorytetem;
- selekcja faktów – manipulator wybiera fakty tylko dla niego wygodne, używa sloganów i pozwala odbiorcom na dostęp tylko do jego przekazów;
- zdanie większości – psychotechnik wmawia odbiorcy, że jego zdanie podziela większość i argumentuje, że wszyscy „zainteresowani” tak mówią;
- kłamstwo – oferent po prostu kłamie – stara się jednak uprawdopodobnić swoje twierdzenia i ogranicza dostęp odbiorcy do innych źródeł informacji, łączy kłamstwa z faktami;
- prowokacja, presja – wywołanie silnych emocji lub reakcji emocjonalnej – odwraca uwagę od rzeczowych argumentów na rzecz emocji;
- pułapka znikającej szansy (przynęty) – oferent przedstawia podmiotowi manipulacji sytuację, w której szansa na wykorzystanie okazji jest przemijająca i może zostać definitywnie utracona;
- imadło – dokręcanie śruby – stopniowe zwiększanie presji na osobę;
- społeczny dowód słuszności – wykorzystuje tendencje do naśladowania zachowań, zwłaszcza w niepewnych sytuacjach;
- efekt wabika – początkowa prezentacja taniej oferty w konsekwencji okazuje się znacznie droższa, gdyż obarczona jest wieloma warunkami dodatkowymi;
- reguła autorytetu – wykorzystanie pozycji lub wiedzy specjalistycznej do przekonania innych – opinie te traktowane są wówczas jako bardziej wiarygodne i przekonujące.

10.4. Młodzi ludzie – wyzwania, potencjał, a jednak zagrożenie

Pozytywne aspekty

- błyskawiczny dostęp do wiedzy,
- przyspieszenie edukacji ale też maksymalizacja ułatwień, prowokujące „umysłowe lenistwo”,
- rozwój nowych form kreatywności,
- rozwój kompetencji cyfrowych.

Zagrożenia podstawowe

- wsparcie przy wykonywaniu zadań, czytaj – ryzyko „wyłączenia myślenia”, wyboru najłatwiejszej ścieżki, braku kreatywności i spadku samodzielności,
- uzależnienie od generowanych odpowiedzi,
- osłabienie krytycznego myślenia, pseudo emocjonalne treści i obrazy,
- fałszywe narracje,
- wypaczenie opinii, poprzez kontakt z halucynującymi modelami bez wystarczającej edukacji i umiejętności krytycznego myślenia.

To może prowadzić do nowych form nierówności intelektualnych.

Zagrożenia krytyczne

- zanik krytycznego myślenia, podatność na komunikaty typu „deepfake” w kampaniach nienawiści,
- powszechność fałszywych opinii i fake newsów,
- generowane i odrealnione treści pornograficzne oraz propagowanie poniżających, wulgarnych, niehumanitarnych i niegodnych zachowań,
- fałszywe narracje i komentarze,
- polityczna manipulacja,
- radykalizacja zachowań w kierunku skrajnych opinii społecznych.

10.5. Martwy Internet

Teoria spiskowa dowodząca i opisująca sytuację, wg której ponad 50% treści w Internecie generowane jest przez boty (skrypty) oparte na modelach językowych generatywnej AI.

Manipulacja treścią jest wykorzystywana do kontroli populacji i ograniczania naturalnej aktywności ludzi. Zwolennicy tej teorii wierzą, że te boty społecznościowe zostały celowo stworzone, aby manipulować algorytmami i poprawiać wyniki wyszukiwania w celu wpływania na ludzi lub na ich wybory, również społeczne i polityczne.

Fakty: teoria martwego Internetu zyskała na popularności, ponieważ wiele obserwowanych zjawisk można wiarygodnie zmierzyć, m.in. takich jak zwiększony ruch botów i wpływ algorytmów na moderowanie i promowanie określonych treści.

10.6. Manipulacja faktami, w której wykorzystywane jest AI

Manipulacja faktami, popularne techniki:

Spin:

- prezentowanie faktów w sposób, który sugeruje, że są one korzystne dla danej osoby lub organizacji, nawet jeśli w rzeczywistości tak nie jest.

Gaslighting:

- technika manipulacji, w której ofiara jest przekonywana, że jej percepcja rzeczywistości jest błędna lub nieprawdziwa.

Dezinformacja:

- celowe rozpowszechnianie fałszywych informacji, aby wprowadzić w błąd opinię publiczną.

Manipulacja mediami:

- wykorzystywanie środków masowego przekazu do kształtowania poglądów i postaw ludzi.

Jak się bronić przed manipulacją faktami:

- krytyczne myślenie: analizuj informacje z różnych źródeł i zadawaj pytania, zamiast ślepo wierzyć w to, co czytasz, widzisz lub słyszysz – fakt; nie jest to łatwe...

Sprawdzanie faktów:

- Upewnij się, że informacje, które otrzymujesz, są potwierdzone przez wiarygodne źródła. Szukaj też wsparcia i opinii osób, którym ufasz, jeśli czujesz że jesteś manipulowany.

Rozpoznawanie własnych emocji:

- Bądź świadomy, że manipulacja często opiera się na emocjach, a nie na faktach. Manipulacja opiniami często polega na wykorzystywaniu zaufania i budowaniu fałszywego poczucia bezpieczeństwa.

Rozwój asertywności:

- Umiejętność odmawiania i wyrażania swojego zdania, jest to bardzo ważna cecha w obronie przed manipulacją. Unikaj pochopnego podejmowania decyzji, szczególnie pod wpływem silnych emocji lub presji.

Świadomość własnych słabości:

- Przekonanie odbiorcy, że osoby z niskim poczuciem własnej wartości lub brakiem asertywności są bardziej podatne na manipulację. Nie daj się poddać presji czasu lub sytuacji, w sytuacji w której czujesz się naciskany do podjęcia decyzji, z którą czujesz się niekomfortowo – odpuść, wstrzymaj się!

Dodatkowe wskazówki:

- Myśl i bądź czujny...

10.7. Możliwe punkty krytyczne

Najważniejsze „punkty zwrotne”:

- powstanie AGI (Artificial General Intelligence),
- pełna automatyzacja pracy umysłowej,
- integracja AI z systemami militarnymi,
- kryzys zaufania do źródeł informacji.

10.8. Demokracje — AI jako narzędzie oraz jako zagrożenie

AI zmienia:

1. Informacje, przekaz publiczny i edukacja młodych

- deepfake’i, manipulacje, propaganda,
- automatyzacja produkcji fałszywych treści,
- personalizację przekazu politycznego.

2. Procesy demokratyczne

- ryzyko koncentracji władzy w rękach właścicieli modeli i architektów algorytmów,
- zagrożenie nierównowagą informacyjną,
- zasadnicza trudność regulowania i nadzoru algorytmów globalnych systemów AI.

3. Procesy edukacyjne

- ułatwienie pisania wypracowań, rozwiązywanie zadań i przygotowywanie prezentacji,
- zmniejszenie samodzielności uczniów i ograniczenie przyszłych kompetencji,
- powszechne wykorzystanie AI prowadzi do powierzchownego rozumienia, zastępuje myślenie łatwością uzyskania „gotowych odpowiedzi”.

4. Sferę obywatelską

- możliwość automatycznego monitorowania obywateli,
- wpływ dużych platform na opinię publiczną.

10.9. Chiński pokój... – ważny eksperyment myślowy

Eksperyment myślowy zaproponowany przez amerykańskiego filozofa Johna Searle'a i przedstawiony w jego pracy z 1980 roku pt. „*Minds, Brains, and Programs*” mający pokazać, że nawet skuteczne symulowanie rozumu przez komputer nie jest tożsame z posiadaniem prawdziwego rozumu przez, nawet zaawansowaną maszynę, ponieważ wykonywanie określonych zadań (np. obliczeniowych) nie musi opierać się na rozumieniu ich przez wykonawcę. Służy on jako argument przeciwnikom teorii tzw. silnej sztucznej inteligencji i obliczeniowej teorii umysłu. U podstaw eksperymentu stoi niezgodność między syntaksą a semantyką.

Argument chińskiego pokoju odnosi się tylko do programów, które są wykonywane na komputerowych maszynach cyfrowych, i nie są aplikowane do ogólnych maszyn a sam argument jest tematem krytyki ze strony filozofów umysłu i naukowców AI[

Koncepcja eksperymentu

Założmy, że skonstruowaliśmy komputer, który zachowuje się tak, jakby rozumiał język chiński. Innymi słowy, komputer bierze chińskie znaki jako podstawę wejściową i śledzi zbiór reguł nimi rządzący, koreluje je z innymi chińskimi znakami, które prezentuje jako informację wyjściową.

Założmy, że ten komputer wykonuje to zadanie w sposób tak przekonujący, że łatwo przechodzi Test Turinga, tzn. przekonuje Chińczyka, że jest Chińczykiem. Na wszystkie pytania, które człowiek zadaje, udziela właściwych odpowiedzi w sposób tak naturalny, że Chińczyk jest przekonany, iż rozmawia z innym Chińczykiem. Zwolennicy mocnej sztucznej inteligencji wyciągają stąd wniosek, że komputer rozumie chiński tak, jak człowiek.

Teraz filozof John Searle proponuje, żeby założyć, iż to on sam siedzi wewnątrz komputera. Innymi słowy, On Sam znajduje się w małym pokoju, w którym dostaje chińskie znaki, konstruuje książkę reguł, a następnie zwraca inne chińskie znaki, ułożone zgodnie z tymi regułami. Searle zauważa, że oczywiście nie rozumie ani słowa po chińsku, mimo iż wykonuje powierzone mu zadanie. Następnie argumentuje, że jego brak rozumienia dowodzi, że i komputery nie rozumieją chińskiego, znajdując się w takiej samej sytuacji jak On: są bezumysłowymi manipulatorami symboli i nie rozumieją, co „mówią”, tak jak i On nie rozumie treści chińskich znaków, którymi operował.

Eksperyment

W ciągu ostatnich dwóch dekad XXI wieku argument chińskiego pokoju był przedmiotem wielu dyskusji. W 1984 Searle zaprezentował argument chińskiego pokoju w książce pt. *Mind, Brains and Science*. W styczniu 1990 roku popularny periodyk „Scientific American” przedstawił debatę na ogólnym forum naukowym. Searle włączył argument chińskiego pokoju w swą wypowiedź zatytułowaną „*Is the Brain's Mind a Computer Program?*”. Odpowiedzią był artykuł *Could a Machine Think?* napisany przez Paula i Patricję Churchlandów. Wkrótce potem opublikowana została dyskusja Searle'a o chińskim pokoju z innym wiodącym filozofem umysłu, Jerryem Fodorem.

Sercem argumentu jest wyobrażona ludzka symulacja komputera podobna do Papierowej Maszyny Turinga. Człowiek w chińskim pokoju przestrzega angielskich instrukcji dla manipulowania chińskimi znakami, gdzie komputer „przestrzega” programu napisanego w języku

obliczeniowym. Człowiek produkuje podobieństwo rozumienia chińskiego przez przestrzeganie instrukcji manipulacji symbolami, ale nie dochodzi przez to do rozumienia chińskiego. Ponieważ komputer robi to, co robi człowiek – jedynie manipuluje symbolami na podstawie ich składni – żaden komputer nie może dojść do istotnego rozumienia języka chińskiego wyłącznie przez przestrzeganie programu.

Ten ściśle oparty na scenariuszu chińskiego pokoju argument jest skierowany przeciw stanowisku nazwanemu przez Searle’a „*Mocną AP*”. Wg niego „*Mocna AP*” jest postulatem, że odpowiednio zaprogramowane komputery (albo same programy) mogą rozumieć naturalny język i mieć inne zdolności mentalne podobne do ludzkich, których możliwości one naśladują. Nawiązując do mocnej AI, komputer może inteligentnie grać w szachy, robić bystre ruchy albo rozumieć język. Przez kontrast słaba AI („*Weak AP*”) jest poglądem, że komputery są tylko użyteczne w psychologii, lingwistyce i po części w innych obszarach, ponieważ mogą symulować zdolności mentalne. Ale słaba AI nie twierdzi, że komputery rozumieją albo są inteligentne. Argument chińskiego pokoju nie jest skierowany w słabą AI, ani nie ma na celu pokazania, że maszyny nie mogą myśleć – Searle postuluje, że ludzki mózg również jest maszyną i mimo to ma zdolność myślenia. Argument ten ma podważać pogląd, że formalne wyliczenia na symbolach produkują myśl.

Argument I

Przeciw mocnej AI możemy wyciągnąć jako *reductio ad absurdum* taki argument: (niech L będzie naturalnym językiem i powiedzmy, że „program dla L” jest programem dla płynnego rozmawiania w L. System komputerowy jest dowolnym systemem – może być nim człowiek lub coś innego, co może wykonywać program). Jeżeli mocna AI jest prawdziwa to istnieje taki program dla L, dzięki któremu, jeśli dowolny komputer wykonuje ten program, system dojdzie do rozumienia L. Mogę wykonać program dla L bez rozumienia L.

Te dwa wnioski ukazują, że mocna AI jest fałszywa.

Argument II

Druga przesłanka jest wspierana przez myślowy eksperyment chińskiego pokoju. Konkluzją argumentu jest, że uruchomienie programu nie może stworzyć rozumienia. Szerszy argument zawiera stwierdzenie, że myślowy eksperyment pokazuje ogólnie, że nikt nie może otrzymać semantyki (znaczenia) z syntaksy (formalnego manipulowania symbolami).

Jądrem argumentu Searle’a jest rozróżnienie między syntaksą i semantyką. Pokój jest w stanie przedstawiać litery zgodnie z książką reguł. To znaczy, że zachowanie pokoju może być opisane jako postępujące z regułami syntaktycznymi. Ale w stanowisku Searle’a on sam nie zna znaczenia, tego co robi. To znaczy, że nie ma treści semantycznej. Znaki nie są nawet symbolami, bo nie są interpretowane na żadnym etapie procesu.

10.10. Model Elona Muska a demokracja

Elon Musk promuje model demokracji oparty na:

- absolutnej wolności słowa, graniczącej ze skrajną głupotą (w tym nieodpowiedzialne popieranie np. skrajnych opinii Adolfa Hitlera),

- minimalnej moderacji treści,
- decentralizacji władzy informacji,
- „odfiltrowaniu” wpływu instytucji państwowych na platformy społecznościowe.

Musk przejął kontrolę nad jedną z największych sieci komunikacji politycznej (X, dawniej Twitter). Konsekwencje:

- większa swoboda wypowiedzi,
- jednocześnie większa podatność na manipulację, dezinformację i skrajności,
- wpływ na globalne debaty polityczne,
- redefinicja roli platform jako podmiotów politycznych.

Elon Musk, poprzez dysponowanie olbrzymim budżetem, wpływami i powiązaniem z obecną władzą USA oraz niekonwencjonalnym myśleniem o współczesnym świecie (przypominam – choroba Aspergera, ograniczone spektrum autyzmu Muska), łączy wpływ technologiczny, informacyjny i polityczny w jeden „szczytny” cel – odkłamanie Świata, mimo wszystko. Czyni go to jedną z kluczowych postaci współczesnego krajobrazu demokratycznego, bazującego i opartego na masowej psychologicznej analizie zachowań oraz nieograniczonej dostępności informacji i precyzyjnej analizie wielkich zbiorów danych cyfrowych.

11. SCENARIUSZE PRZYSZŁOŚCI – NADZIEJE, OBAWY I MOŻLIWE DROGI ROZWOJU AI

11.1. Scenariusz pierwszy: OPTYMISTYCZNY

Świat wybiera model etycznej AI:

- rozwój edukacji cyfrowej,
- regulacje BigTechów,
- współpraca międzynarodowa.

Skutki:

- wyższy poziom dobrobytu,
- automatyzacja pracy zmniejsza nierówności,
- AI pomaga w nauce, zdrowiu, ekologii.

11.2. Scenariusz drugi: REALISTYCZNY

AI staje się trwałym elementem codzienności:

- praca hybrydowa człowiek – model,
- automatyzacja części zawodów,
- wzrost wpływu korporacji,
- konflikty społeczne pozostają.

Państwo algorytmiczne – realne przyszłe ryzyko – jeśli państwa rozpoczną:

- „legalną” analizę zachowań i opinii obywateli poprzez wykorzystanie specjalizowanych AI,
- analizę, przewidywanie i predykcję zachowań społecznych,
- personalizowanie polityki,
- przekształcenie demokracji w nową formę autorytaryzmu.

11.3. Scenariusz trzeci: PESYMISTYCZNY

AI prowadzi do:

- dezinformacji masowej,
- upadku zaufania publicznego,
- monopolizacji i komercjalizacji wiedzy,
- nieodwracalnego kryzysu demokracji.

Skutki, scenariusz „post-ludzkiego chaosu”, o którym ostrzegają:

- Stuart Russell,
- Geoffrey Hinton,
- Yoshua Bengio.

12. PREDYKCJE WYNIKAJĄCE Z TEJ HISTORII

- Modele AI będą łączyć logikę, probabilistykę i reprezentacje głębokie.
- AI przyczynowa (Pearl) stanie się fundamentem przyszłych systemów bezpiecznych.
- Społeczeństwa demokratyczne będą wymagały nowych instytucji i regulacji.
- Młodzi ludzie będą musieli rozwijać meta-kompetencje: krytyczne myślenie, etykę, rozumienie technologii.
- AI stanie się współtwórcą procesów politycznych i zachowań społeczeństw demokratycznych.

GENESIS, NA KOŃCU...

Corpus delicti

- łacińskie „*corpus*” – ciało, rdzeń, „*delicti*” – przestępstwo, zbrodnia,
- „*corpus delicti*” to łacińskie wyrażenie, które w dosłownym tłumaczeniu oznacza m.in. „ciało przestępstwa”,
- w kontekście prawnym odnosi się do zasady, że nie można kogoś skazać za przestępstwo bez dowodu, że to przestępstwo faktycznie miało miejsce.
- innymi słowy, potrzebne są dowody na to, aby przypisać danej osobie czyn przestępczy, który rzeczywiście miał miejsce, a nie tylko że ktoś go zrelacjonował.

Wg polskiego tłumaczenia naukowców Uniwersytetu Wrocławskiego, Ewy Banaszak i Pawła Czajkowskiego, to „rozkoszne ciało”...

Informare

- łacińskie „*informare*” – kształtować, wyobrażać, określać...,
- komunikat, w szczególności: wypowiedź, tekst wiadomości, opis,
- opis stanu – zestaw informacji, który potocznie dla celów informatyki nazwalibyśmy „danymi”.

Alucinari

- od łacińskiego czasownika „*alucinari*” – halucynacje, błądzenie w umyśle lub bredzenie, majaczenie...,
- to zjawisko polegające na tym, że modele językowe sztucznej inteligencji generują informacje, które są nieprawdziwe, nieistniejące lub niezwiązane z danymi wejściowymi,

- halucynacje powstają często na skutek błędnej interpretacji danych treningowych, niewystarczającej ilości niezweryfikowanych źródeł danych lub złożoności algorytmów,
- powstają także z powodu przeprowadzonego uczenia maszynowego na podstawie ogromnych zbiorów danych, w tym zbiorów kreatywnych (poezja, literatura, baśnie itp.) lub źródeł stronicznych, jak teorie spiskowe (np. teoria płaskiej ziemi),
- modele AI powstały by generować spójne i wiarygodne odpowiedzi, zatem gdy napotykają lukę informacyjną, mogą generować możliwie prawdopodobną lecz fikcyjną kontynuację treści.

Taki przekaz prowadzi do rozpowszechniania fałszywych informacji

Mendacium, mentiri

- łacińskie „*mendacium*”, „*mentiri*”, „*mendax*” – kłamliwy, kłamca, oszukańczy...,
- kłamcy patologiczni oszukują ludzi dla satysfakcji a także w celu uzyskania korzyści, np. kłamca opowiada historie, które stawiają go w innym, korzystniejszym świetle...

Fraud, deceptio

- oszustwo jest przestępstwem skutkowym – skutkiem oszustwa jest niekorzystne rozporządzenie majątkiem własnym lub cudzym, najczęściej wywołanie niekorzystnej dla pokrzywdzonego decyzji rozporządzającej w odniesieniu do jego mienia,
- modele AI powstały by generować spójne i wiarygodne odpowiedzi, zatem gdy napotykają lukę informacyjną, mogą generować możliwie prawdopodobną lecz fikcyjną kontynuację treści.

Falsum

- łacińskie „*falsum*” – fałsz...
- nieprawdziwy komunikat, opinia – nieprawda powiedziana świadomie, mająca na celu wprowadzenie kogoś w błąd.

ZAKOŃCZENIE

Historia AI jest historią współpracy pokoleń naukowców i wynalazców

Jej rozwój od Einsteina, von Neumanna, Turinga i Shannona po Sutskevera, Hintona i Russella był możliwy tylko dzięki postępowi technologii, matematyki, rozwiązań sprzętowych i edukacji społeczeństw, które te rozwiązania tworzą, przekształcają i adoptują.

Powiedzieć, że AI jest jedynie technologią, to za mało. To kompleksowy fenomen obejmujący naukę, inżynierię, politykę, socjologię i kulturę. Wszystkie wymienione postaci a także bardzo wielu ludzi, nie wymienionych z nazwiska stworzyło technologie, fizyczne podstawy i dało koncepcyjne podstawy AI. Następcy doprowadzili do praktycznego rozkwitu technologii a krytycznie myślący naukowcy (Pearl, Russell i inni) wprowadzili konieczne pytania o przyczynowość, „groźną” autonomiczność i nasze bezpieczeństwo.

AI jest największą rewolucją od czasu wynalezienia druku przez Gutenberga:

- poszerza i tworzy nową wiedzę,
- zmienia pracę,
- zmienia kulturę,
- zmienia relacje,

- kształtuje zachowania społeczne i demokrację,
- zmienia politykę.

Dziś AI nie jest już tylko narzędziem nauki – stała się siłą kształtującą sposób myślenia młodych ludzi, strukturę demokracji, politykę informacji i przyszły kształt cywilizacji.

Krytyczne wyzwania na dziś:

Władza nad technologią AI jest w rękach nielicznych, najwięksi gracze:

- BigTech (Google, Meta, Microsoft, Amazon),
- państwa autorytarne (Chiny),
- kilkunastu naukowców, którzy tworzą modele,
- miliarderzy (Musk, Trump, Zuckenberg, Bezos itd.).

To rodzi ogromne ryzyka: halucynacje modeli, energetyczność treningów, zagrożenie prywatności danych, asymetria władzy informacyjnej i wpływ na rozwój młodych ludzi oraz stabilność demokracji.

Co dalej:

technicznie – rozwój modeli przyczynowych i hybrydowych;

politycznie – regulacje i audytowalność;

społecznie – edukacja medialna i rozwój kompetencji empatycznych.

Młodzież jest najbardziej zagrożoną grupą, AI wpływa na:

- rozwój mózgu,
- emocje,
- samopoczucie,
- edukację,
- relacje.

Obok małych dzieci, to najbardziej delikatna i wrażliwa część społeczeństwa.

Przyszłość AI jest otwarta i zależy od nas

Możemy stworzyć:

- lepszą cywilizację,
- bardziej demokratyczny świat,
- bardziej inteligentne społeczeństwo.

Naszym zadaniem jest stworzyć AI, która nie zniszczy człowieka.

Postulujemy wprowadzenie głównych zasad:

- regulacje,
- edukacja,
- transparentność,
- etyka,
- odpowiedzialność,
- nadzór publiczny.

Ale możemy też:

- podzielić świat,
- zniszczyć zaufanie,
- utracić kontrolę nad technologią.

To my zdecydujemy, w którą stronę pójdzie ta historia.

Rozumienie genezy powstawania AI pozwala częściowo przewidywać jej przyszłość.

BIBLIOGRAFIA (WYBRANE KLUCZOWE ŹRÓDŁA)

Fundamenty matematyczne i informatyczne

1. Turing, A. (1936). *On Computable Numbers, with an Application to the Entscheidungs-problem*.
2. Turing, A. M. (1950). *Computing Machinery and Intelligence*. Mind.
3. Shannon, C. (1948). *A Mathematical Theory of Communication*. Bell System Technical Journal.
4. Einstein, A. (1905–1916). *On a Heuristic Viewpoint Concerning the Production and Transformation of Light* (zestaw prac dotyczących efektu fotoelektrycznego i teorii względności).

Początki AI i sieci neuronowych

5. McCarthy, J. (1956). *Dartmouth Artificial Intelligence Project Proposal*.
6. McCarthy, J. (1960). *Recursive Functions of Symbolic Expressions and Their Computation by Machine*.
7. Rosenblatt, F. (1958). *The Perceptron: A Probabilistic Model for Information Storage and Organization in the Brain*.

Teoria probabilistyczna

8. Pearl, J. (1988). *Probabilistic Reasoning in Intelligent Systems*.
9. Pearl, J. (2009). *Causality: Models, Reasoning and Inference*.

Głębokie uczenie i architektury

10. Hinton, G. (2006–2012).
11. Hinton, G., Osindero, S., & Teh, Y. (2006). A Fast Learning Algorithm for Deep Belief Nets.
12. Krizhevsky, A., Sutskever, I., & Hinton, G. (2012). ImageNet Classification with Deep Convolutional Neural Networks. NIPS.
13. Bengio, Y., LeCun, Y., & Hinton, G. (2015). *Deep Learning*. Nature.
14. Vaswani, A., et al. (2017). Attention is All You Need. (Transformer).

Modele generatywne

15. Sutskever, I., Vinyals, O., & Le, Q. (2014). *Sequence to Sequence Learning with Neural Networks*.
16. Radford, A., Sutskever, I., et al. (2018–2020). *GPT Series Papers*.
17. Radford, A., et al. (2018). Improving Language Understanding by Generative Pre-Training. (GPT-1).
18. Brown, T. B., et al. (2020). Language Models are Few-Shot Learners. (GPT-3).

Przyczynowość, etyka i bezpieczeństwo

19. Pearl, J. (2000). *Causality: Models, Reasoning and Inference*.
20. Russell, S., Norvig, P. (2010). *Artificial Intelligence: A Modern Approach*.
21. Russell, S. (2019). Human Compatible: Artificial Intelligence and the Problem of Control.

Krytyka społeczeństwa informacyjnego a demokracja

22. Zuboff, S. (2019). *The Age of Surveillance Capitalism*.
23. O'Neil, C. (2016). *Weapons of Math Destruction*.

Kiedy ochrona staje się pokusą – Allegro Ochrona Kupujących z perspektywy bezpieczeństwa platformy

„Jeszcze gdy chodziłem do podstawówki, to był tam taki Paweł i ja jechałem na rowerze i go spotkałem i potem jeszcze pojechałem do biedronki na lody i po drodze do domu wtedy jeszcze, już do domu pojechałem” – zapytani o to co ten skądinąd klasyczny tekst robi w niniejszym opracowaniu odpowiemy, że ma on zmienić perspektywę w odniesieniu do systemu rekompensat – jedni użyją go standardowo, inni „kreatywnie”.

Zaufanie jako waluta w handlu internetowym

Zaufanie w handlu internetowym działa jak Wi-Fi. Dopóki łączy, wszyscy są zadowoleni. Kiedy natomiast sygnał znika, natychmiast pojawia się panika, a każdy zaczyna szukać winnych. W Allegro Ochrona Kupujących bywa podobnie. Dopóki wszystko działa, nikt o tym nie myśli. Ale gdy coś pójdzie nie tak, nagle okazuje się, że każdy ma swoją wersję rzeczywistości.

Program Allegro Ochrona Kupujących (wcześniej Allegro Protect, a jeszcze wcześniej Program Ochrony Kupujących) to narzędzie, które każdego dnia chroni tysiące kupujących przed stratą pieniędzy. Jednocześnie jest lustrem ludzkiej pomysłowości. Jeśli komuś wydaje się, że widział już wszystko, powinien spędzić tydzień w naszym zespole. W tym świecie kreatywność nie zna granic.

Ogromna większość wniosków jest oczywiście uczciwa. Ktoś nie otrzymał towaru, coś przyszło uszkodzone, sprzedawca zniknął. Klasyka handlu online. Problemy zaczynają się wtedy, gdy uzasadnienia przestają przypominać rzeczywistość. W rubryce „powód reklamacji” pojawia się coś w rodzaju: „olejek był bezzapachowy, a jednocześnie śmierdział”, „cukier był wilgotny” albo „krem się zważył, więc się obraziłam i chcę zwrot pieniędzy”.

Mechanizm działania programu Allegro Ochrona Kupujących

Program Allegro Ochrona Kupujących (AOK) stanowi kluczowy element systemu bezpieczeństwa platformy Allegro. Jego celem jest zapewnienie kupującemu ochrony finansowej w sytuacjach, gdy transakcja nie zostanie zrealizowana zgodnie z umową zawartą pomiędzy stronami. System ten ma charakter kompensacyjny co oznacza, że w określonych przypadkach środki są zwracane kupującemu bezpośrednio przez Allegro, rzecz jasna po przeprowadzeniu wewnętrznej weryfikacji i ocenie zasadności wniosku.

1. Zakres ochrony

Program obejmuje sytuacje, w których kupujący: zapłacił za towar, ale go nie otrzymał, otrzymał towar niezgodny z opisem lub o znacznie niższej wartości niż deklarowana, otrzymał towar uszkodzony w transporcie, zwrócił towar lub odstąpił od umowy, ale nie otrzymał zwrotu pieniędzy.

W wyjątkowych przypadkach AOK obejmuje także rekompensatę kosztów wysyłki, jeśli zostały poniesione przez kupującego w dobrej wierze, a sprzedawca nie wywiązał się ze swoich obowiązków.

2. Proces weryfikacji wniosku

Procedura w ramach AOK jest wieloetapowa i ma na celu zapewnienie obiektywności decyzji. Każdy wniosek przechodzi następujące etapy:

a) Zgłoszenie problemu i dyskusja ze sprzedawcą.

Pierwszym krokiem jest otwarcie tzw. „dyskusji”, czyli bezpośredniego kanału komunikacji między kupującym a sprzedawcą w obrębie platformy. Dyskusja ma charakter mediacyjny i pozwala stronom samodzielnie rozwiązać spór. W większości przypadków problem udaje się wyjaśnić na tym etapie.

b) Złożenie wniosku o ochronę.

Jeśli sprzedawca nie odpowie, nie podejmie działań naprawczych lub stanowisko stron pozostaje rozbieżne, kupujący może złożyć wniosek w ramach Allegro Ochrona Kupujących. Wniosek składany jest przez dedykowany formularz, w którym użytkownik opisuje sytuację, wskazuje numer oferty oraz dołącza dowody potwierdzające jego roszczenie (np. zdjęcia, korespondencję, potwierdzenia nadania przesyłki).

c) Analiza wstępna.

Na tym etapie weryfikowana jest formalna poprawność zgłoszenia – m.in. czy transakcja faktycznie została zawarta w obrębie Allegro, czy płatność przeszła przez obsługiwane kanały (np. PayU, Allegro Pay), a także czy nie upłynął termin składania wniosków określony w regulaminie.

d) Ocena zasadności roszczenia.

To kluczowy etap, na którym analitycy Allegro dokonują oceny merytorycznej zgłoszenia. Wykorzystywane są tu m.in.:

- dane z historii konta i transakcji,
- zapis komunikacji w ramach dyskusji,
- dokumentacja dostarczona przez kupującego i sprzedawcę,
- informacje od przewoźnika (status przesyłki, potwierdzenie doręczenia, protokoły szkody).

W uzasadnionych przypadkach podejmowana jest również bezpośrednia komunikacja z obiema stronami, aby doprecyzować szczegóły lub uzyskać dodatkowe dowody.

e) Decyzja i wypłata środków.

Po pozytywnej weryfikacji Allegro dokonuje wypłaty środków na rachunek kupującego, pokrywając kwotę transakcji (łącznie z kosztem dostawy, jeśli dotyczy). Wypłata ma charakter jednorazowy i stanowi zamknięcie procedury. Sprzedawca, wobec którego potwierdzono uchybienia, może zostać obciążony konsekwencjami regulaminowymi lub finansowymi.

f) Archiwizacja i analiza ryzyka.

Każdy wniosek, niezależnie od wyniku, trafia do centralnej bazy danych. Dane te służą do identyfikacji powtarzających się schematów, nadużyć oraz potencjalnych powiązań między kontami użytkowników. Wnioski są analizowane pod kątem występowania wzorców językowych, sposobu składania zgłoszeń, typów towarów oraz schematów działania. W przypadku podejrzenia przestępstwa materiały są przekazywane do Zespołu ds. Współpracy z Organami Ścigania (WZOS).

3. Odpowiedzialność i rola Allegro

Warto podkreślić, że Allegro nie jest stroną transakcji między kupującym a sprzedawcą. Rola platformy polega na zapewnieniu przestrzeni do zawierania umów oraz na administrowaniu środkami w ramach systemów płatniczych.

Program Allegro Ochrona Kupujących jest formą dobrowolnej gwarancji, wynikającej z odpowiedzialności społecznej i reputacyjnej, a nie z przepisów o rękojmi czy gwarancji producenta. Oznacza to, że decyzje w ramach AOK są podejmowane w oparciu o analizę danych i ocenę zaufania do stron, a nie wyłącznie o sztywne procedury prawne.

4. Weryfikacja uczciwości i zapobieganie nadużyciom

System AOK został zaprojektowany tak, by łączyć prostotę dla uczciwego użytkownika z wielowarstwową kontrolą dla potencjalnego nadużycia. Wykorzystuje on elementy automatycznej analizy (np. status przesyłki, powtarzalność danych) oraz indywidualną ocenę ekspercką.

Każde zgłoszenie o nietypowym przebiegu – np. seria roszczeń o podobnej treści, identyczne zdjęcia czy zbieżne adresy dostawy – trafia do analityków bezpieczeństwa. W przypadku potwierdzenia nadużycia Allegro może wstrzymać wypłatę, zamknąć konto, a w poważniejszych przypadkach przekazać sprawę Policji wraz z pełną dokumentacją elektroniczną.

5. Współpraca między zespołami

Proces AOK jest efektem współdziałania kilku obszarów organizacyjnych Allegro:

- zespołów obsługi kupujących i sprzedających,
- działu bezpieczeństwa i zaufania,
- działu prawnego,
- zespołu ds. współpracy z organami ścigania (WZOS),

Dzięki temu możliwe jest nie tylko rozwiązywanie indywidualnych spraw, ale też monitorowanie zjawisk i trendów w skali całej platformy.

6. Znaczenie systemowe

Allegro Ochrona Kupujących pełni podwójną funkcję. Z jednej strony chroni użytkowników i utrzuca zaufanie do platformy jako bezpiecznego miejsca handlu. Z drugiej strony jest narzędziem analitycznym, które pozwala wykrywać nowe formy nadużyć, analizować zachowania sprawców i reagować, zanim straty staną się masowe.

Z perspektywy bezpieczeństwa e-commerce program ten można uznać za system wczesnego ostrzegania, każdy wniosek to sygnał, który może ujawnić nie tylko indywidualny spór, lecz także nowy schemat przestępczy.

Niewinne roszczenia czy już oszustwa? – analiza przypadków

Wspomnieliśmy na początku, że wniosek o rekompensatę może być standardowy lub kreatywny. W przypadku tego pierwszego nie ma zbyt dużego pola do tworzenia kwiecistego opowiadania – zamówiłem towar, nie otrzymałem go (ewentualnie otrzymałem plastelinę, cegłę, cukier, itp.).



Fot. 1. Autentyczna przesyłka ze stycznia 2025r., zawierająca gipsowy odlew iPhone, wagowo odpowiadający wadze tegoż aparatu

Sprawca/Sprzedający jest proszony wówczas o wyjaśnienie, jeśli serwis nie otrzyma stosownej wiadomości sprawa jest procedowana przez nasz dział – WZOŚ.

Innym przykładem gdzie nasi Klienci zwracają się po pieniądze jest mniej oczywista, ale ciągle racjonalna justyfikacja:

„– *Zobacz na to konto, ile ono ma aktywnych wniosków? – Kilkanaście*” – wybrzmiał pewnego razu dialog między dwoma agentami, którzy akceptują wnioski o rekompensatę. Po przyjrzeniu się Klientowi okazuje się, że nie próbuje on wyłudzić naszych środków, a odzyskać swoje pieniądze za nie do końca uczciwą ofertę. Jak to możliwe? Niektórzy z naszych Klientów polują na okazje. Najczęściej dotyczy to działu z elektroniką, bo tu o takie najprościej. „*Telefon ma uszkodzony wyświetlacz, prawa strona ekranu jest wyraźnie bledsza, widoczna gorsza jakość obrazu – nie znam się na tym, więc wystawiam, może ktoś sobie to naprawi*”. Cena znacznie niższa niż w detalu, nowy model kosztuje 1500 PLN, a opisywany aparat wystawiono za 750 PLN. Dla kogoś kto naprawia sprzęty GSM jest to bardzo dobra okazja, przecież to tylko

wymiana ekranu, w dodatku można przecież wstawić nieoryginalny i zarobić więcej przy ponownej odsprzedaży „odświeżonego” sprzętu. Po otrzymaniu przesyłki okazuje się, że nie tylko ekran jest uszkodzony. Nie słychać w ogóle rozmówcy, telefon gubi zasięg, ma uszkodzenia obudowy, a na płytkach PCB widać ślady cieczy. Klient zgłasza nieprawidłowości za pośrednictwem dyskusji (rozmowa między Kupującym, a Sprzedającym, gdzie ma możliwość wypowiedzieć się również obsługa Allegro), skrupulatnie opisuje znacznie większe rozmiary uszkodzeń, niż wynikałoby to z opisu Sprzedającego. Co w sprawie mówi ów Sprzedający? – „no przecież wystawiłem telefon jako uszkodzony, więc o co Panu/Pani chodzi?”

Klasycznie, słowo przeciwko słowu – Klient twierdzi, że przedmiot zakupu jest niezgodny z umową, a Sprzedający, że przecież opisał sprzęt jako uszkodzony. Wówczas rozgoryczony transakcją Kupujący występuje do naszego serwisu z wnioskiem o rekompensatę Allegro Ochrona Kupujących. Kto ma rację? Jest stare powiedzenie, że racja jest jak (cztery litery), każdy ma swoją. W przytoczonym przykładzie to Sprzedający nie opisał rzetelnie sprzedawanego przedmiotu. Przy mnogości wniosków, które otrzymujemy należy stwierdzić, że i tak każdy przypadek rozpatrywany jest indywidualnie, w sytuacjach spornych Klient czasem proszony jest o dodatkowe zdjęcia lub konieczną dokumentację, jednak z założenia program ma być prokliencki, zatem przeważnie rekompensata jest skutecznie przyznana i wypłacona na rachunek wskazany przez Klienta.

Istnieje też druga metoda, kreatywna.

Goszcząc w Sanoku na konferencji ZPI 2025 mieliśmy okazję zaprezentować przypadek nieposkromionej kreatywności jednej z naszych Klientek. Przypomnimy tę właśnie sprawę – w naszym WZOSiowym zespole prowadził ją Artur. Kim jest nasza bohaterka?

Aktywną kupującą – intensywność działań od połowy 2024 do wiosny 2025, domniemane miejsce działania: okolice Białegostoku. Za cel obrała sobie szybką kasę z reklamacji i (wówczas jeszcze) Allegro Protect. Poniżej lista powodów, dla których otwierała wnioski o zwrot (pisownia oryginalna):

OLEJEK BUSAJNA

„Olejek po 2 TYG stracił zapach olejek nie pachnie wogle pomarańczą tylko stał się bezwonny strasznie dziwnie śmierdzi”.

KREM DO TWARZY

„Krem na początku ładnie pachniał po kilku dniach stracił zapach po nałożeniu na twarz stał się dziwny roluje się strasznie na twarzy i nie zaprzyjemnie pachnie”.

BIG NATURE ERYTRYTOL

„Cukier mega zrobił się wilgotny w środku wszystkie paczki wyrzuciłam cukier nie nadaje się do spożycia”.

KONCENTRAT NUTRILITE

„Po zastosowaniu całego opakowania zero jakiegokolwiek efektu pieniądze zmarnowane w błoto.”

SIATKA OGRODZENIOWA

„Siatka na początku była ok ale przyszedł deszcz wiatr wszystko porozrywało mimo tego że nie żałowałam z Mężem trefetek”.

CHUSTECZKI PAMPERS

„Dostała się pleśń w środku opakowań resztę opakowań zostały wyrzucone”

KURKUMA C3 KOMPLEX

„Zero efektu nadal stan zapalny się utrzymuje a kurkuma miała pomóc”

UTSUKUSY KREM DO TWARZY

„Krem niestety mi się zwazył zrobiły się grudy nie tego się spodziewałam”

ZESTAW DO WYRÓWNYWANIA CIŚNIENIA W UCHU

„Córka zaczęła dmuchać baloniki i zaczęły pękać
(...)jak baloniki popękały odrazu zosty wyrzucone”

KAWA JACOBS BARISTA

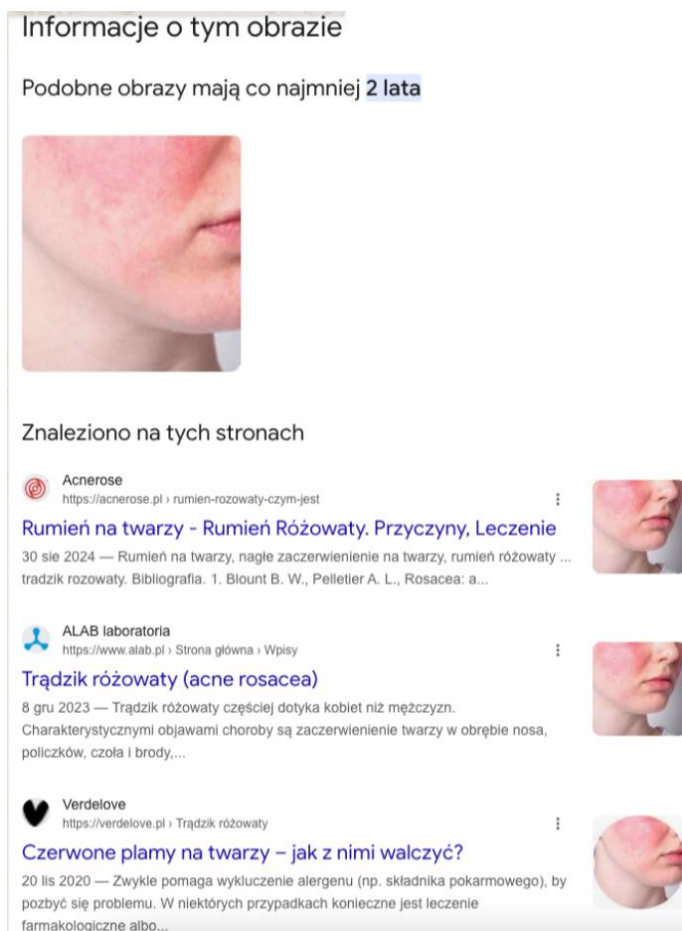
„odebrałam 3 kawy rozpuszczalne i 1 puszka jedna jest pusta”

ARKANA ŻEL DO TWARZY

„żel strasznie piecze mnie twarz po niej wysyłam zdjęcie jak zostałam oszpecona dziwny wogle ten żel”



Fot. 2. Zdjęcie przesłane jako dowód,
że zastosowany żel spowodował
oszepecenie twarzy



Fot. 3. Wynik wyszukiwania obrazem w przeglądarce
Google

Zmiana taktyki

W większości przypadków nadużycia w ramach Allegro Ochrona Kupujących zaczynają się niewinnie. Na początku pojawiają się reklamacje dotyczące jakości towaru np. krem, który „zważył się”, olejek, który „stracił zapach”, czy suplement, który „nie zadziałał”. Choć brzmi to absurdalnie, takie zgłoszenia rzadko są celem samym w sobie. Dla niektórych użytkowników stanowią raczej etap testowania systemu. To moment, w którym sprawdzają, jak daleko mogą się posunąć, zanim ktoś zacznie zadawać pytania.

Kiedy kolejne wnioski nie przynoszą oczekiwanych rezultatów, pojawia się zmiana strategii. Zgłaszający zaczynają tworzyć bardziej dopracowane scenariusze a zatem zamiast spornego zapachu czy konsystencji, pojawia się motyw „*pustej paczki*” albo „*uszkodzenia w transporcie*”. To bardziej wiarygodne i trudniejsze do zweryfikowania formy zgłoszeń.

Charakterystycznym elementem takich przypadków jest sposób, w jaki są one konstruowane. Towar rzekomo nigdy nie dotarł lub po prostu paczka była „pusta”, ale jednocześnie nie ma żadnej możliwości weryfikowania nagrań z momentu odbioru, ponieważ kupujący nie otwiera przesyłki przy paczkomacie. Robi to dopiero w samochodzie lub w domu, a więc tam, gdzie nie ma świadków ani kamer. To świadomy wybór. Z punktu widzenia analityka bezpieczeństwa jest to sygnał ostrzegawczy: sytuacja, w której dowody pojawiają się tylko po stronie zgłaszającego, a każdy obiektywny ślad zniknął, nie jest przypadkowa.



W takich sprawach szczególnie ważna staje się analiza spójności relacji i powtarzalności zachowań. Osoba, która raz zgłosiła pustą paczkę, często robi to ponownie, zmieniając tylko typ towaru a czasem miejsce odbioru. Pojawiają się te same schematy językowe, podobne godziny logowań, te same wzorce w komunikacji ze sprzedawcami. Z pozoru różne przypadki zaczynają tworzyć logiczną całość.

Zmiana taktyki często idzie w parze ze wzrostem pewności siebie. Początkowo zgłaszający pisze niepewnie, ostrożnie, prosząc o pomoc. Po kilku „udanych” reklamacjach ton staje się bardziej stanowczy, czasem wręcz agresywny. „Proszę natychmiast zwrócić pieniądze”, „nie interesuje mnie procedura”, „już zgłosiłam na Policję”. To typowe zwroty, które mają nadać sprawie pozory oficjalności.

Z perspektywy Allegro Ochrona Kupujących jest to moment, w którym rola analityka zmienia się z mediatora w śledczego. Nie chodzi już o rozstrzygnięcie sporu handlowego, lecz o ustalenie czy mamy do czynienia z pomyłką czy z celowym działaniem. Pomagają w tym dane: historia konta, analiza wcześniejszych reklamacji, analiza powiązań, raporty przewoźników. W przypadkach, gdy pojawia się więcej niż jeden wniosek z podobnym schematem, uruchamiane są procedury bezpieczeństwa i współpraca między zespołami Allegro, a w razie potrzeby również z organami ścigania.

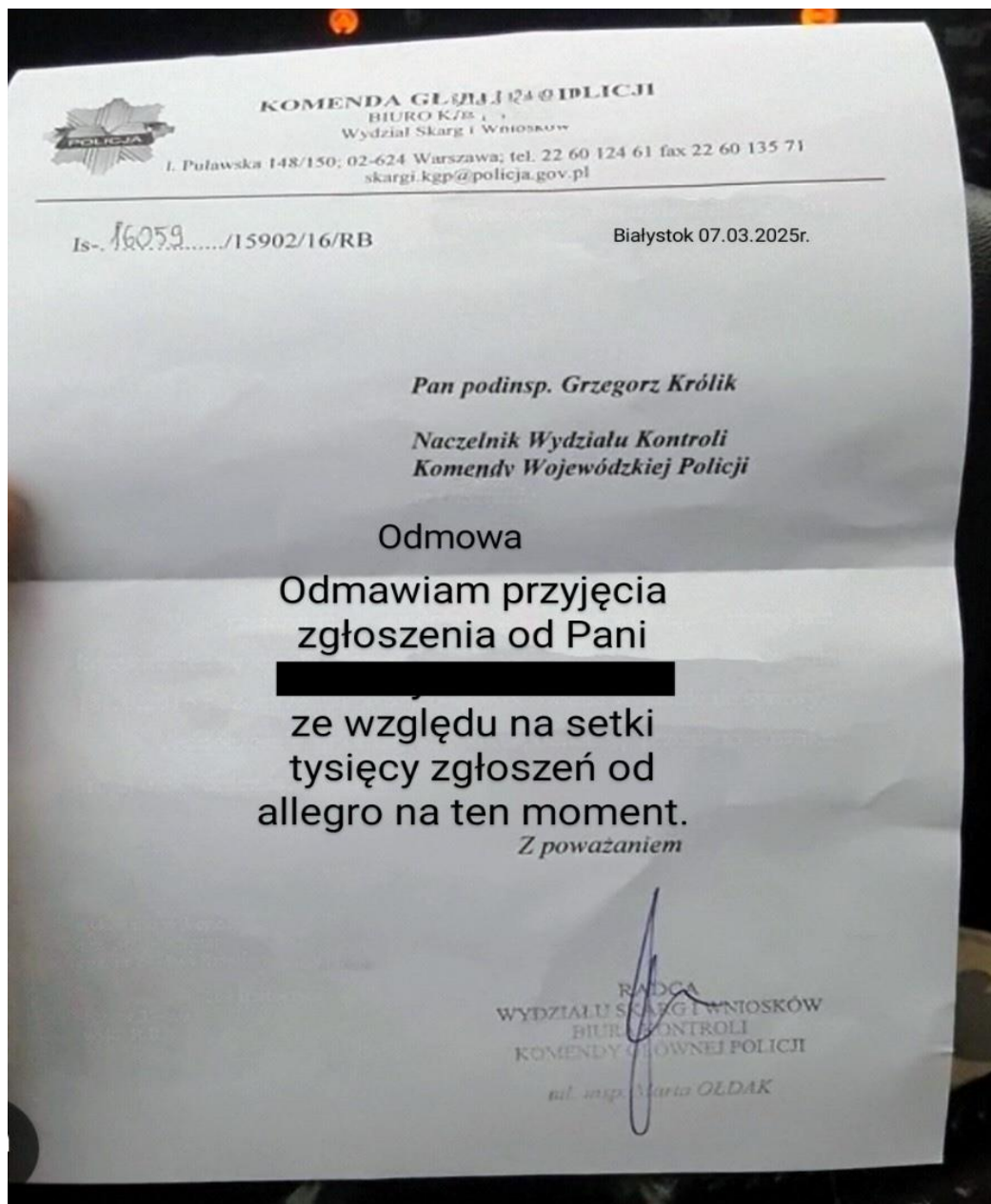
Tego typu zgłoszenia są szczególnie niebezpieczne, bo pozornie mieszczą się w granicach zdrowego rozsądku. Nie ma już przesadzonych opisów typu „olejek śmierdział, bo nie pachniał”. Jest za to poważny ton i dobrze dobrane argumenty. To sprawia, że weryfikacja staje się trudniejsza, a jednocześnie bardziej wymagająca.

Zmiana taktyki pokazuje też, jak elastyczni potrafią być sprawcy nadużyć. Uczą się procedur, poznają język komunikacji konsultantów, powołują się na znane im fragmenty regulaminów. Potrafią zbudować zgłoszenie w taki sposób, by wyglądało jak modelowy przypadek uczciwego klienta. Różnicę widać dopiero po czasie zwłaszcza w liczbie wniosków od jednej osoby, w stylu ich pisanie i w tym, że „problemy” pojawiają się zawsze w podobnych okolicznościach.

Można więc powiedzieć, że na tym etapie Allegro Ochrona Kupujących staje się dla nich nie tylko systemem wsparcia, lecz także swoistym poligonem doświadczalnym. Tam, gdzie uczciwy użytkownik widzi zabezpieczenie, oni widzą pole do eksperymentu. I to właśnie w tych momentach widać, że Ochrona, która miała być pomocą, potrafi stać się pokusą.

Ponowna Zmiana Taktyki

W toku kolejnych spraw związanych z wnioskami o wypłatę środków z programu AOK otrzymaliśmy od zgłaszającej zestaw materiałów mających potwierdzać jej roszczenia: dokumenty w formacie PDF rzekomo będące „potwierdzeniem zgłoszenia na Policję” z nagłówkiem jednostki, pieczętą, podpisem i równoczesną odmową przyjęcia zgłoszenia



Fot. 5. „Odmowa przyjęcia zgłoszenia” z Komendy Głównej Policji – Białystok, 07.03.2025

Powyżej pismo na blankiecie „Komenda Główna Policji – Biuro KGP, Wydział Skarg i Wniosków”, adres warszawski, w treści „odmawiam przyjęcia zgłoszenia (...) ze względu na setki tysięcy zgłoszeń od allegro”, podpis i pieczęć.

Czerwone flagi: Jednostka centralna (KGP, Warszawa) vs miejsce sporządzenia „Białystok”; jest tutaj sprzeczność organizacyjna. Absurdalna podstawa odmowy („setki tysięcy zgłoszeń z Allegro”) – policja rzecz jasna nie odmawia wszczynania tylko z powodu liczby spraw. Styl i język niezgodny ze wzorcami pism policyjnych; układ i typografia wyglądają na skład „amatorski”.

Pieczęć i podpis wyglądają jak wklejone; widoczne różnice rozdzielczości elementów. Wniosek jest oczywisty: pismo przygotowane ad hoc, by uwiarygodnić rzekomą wizytę na Policji; wysoki poziom prawdopodobieństwa fałszu.

RPD-2865460125
(sygn. akt postępowania)

POSTANOWIENIE NR 2865493/25

Komenda Powiatowa w Białymstoku
(oznaczenie wydającego postanowienie)

z dnia 31.08.24 r.

o odmowie przyjęcia odwołania/zażalenia^{*)}

Na podstawie art. 135k ust. 3 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2011 r. Nr 287, poz. 1687, ze zm.)

postanawiam

odmówić przyjęcia odwołania od orzeczenia zakup przez allegro
(oznaczenie przełożonego dyscyplinarnego)

nr 313485 z dnia 31.08.24 r. wydanego w postępowaniu dyscyplinarnym przeciwko
Kier. Ochocko Prędkość 7 04-688 Warszawa
(stopień, imię i nazwisko obwinionego)

obwinionemu o popełnienie przewinienia(-nien) dyscyplinarnego(-nych) określonego(-nych)
W (kwalifikacja przynajmniej jednego zarzutu bądź zarzutów)

ze względu na to, że odmawiamy przyjęcia zgłoszeń. Wskazaliśmy allegro ze względu na bardzo dużą
zgodność tego typu. (przebiegła opinia z art. 135k ust. 3 ustawy o Policji)

Uzasadnienie
Allegro ma obowiązek przyjąć zgłoszenia odmowy przyjęcia z Policji i z Państwa Ludności
kt. str. 51 osobisty allegro przedt. ma obowiązek wypłacić posiłkowe. niekiedy
nie jako zasada obywatela
26.08.2025. Kierownik Ochocko
(stopień, imię i nazwisko, podpis)

Pouczenie

Niniejsze postanowienie jest ostateczne. Obwiniony może zaskarżyć je do Wojewódzkiego Sądu Administracyjnego w (miejscowość)

za pośrednictwem (oznaczenie wyższego przełożonego dyscyplinarnego) w terminie 30 dni od dnia doręczenia postanowienia.

^{*) Niepotrzebne skreślić.}

© www.signform.pl Sp. z o.o., producent aktywnych formularzy, e-mail: biuro@signform.pl

Fot. 6. Postanowienie o odmowie przyjęcia odwołania/zażalenia

Co widzimy: formularz z tytułem „Postanowienie o odmowie przyjęcia odwołania/zażalenia”, powołanie na art. 135k ustawy o policji (przepisy dyscyplinarne), odręczne dopiski „zakup przez allegro”, „odmawiamy przyjęcia zgłoszeń (...) z Allegro”, „Allegro ma obowiązek przyjąć zgłoszenie i wypłacić”.

Czerwone flagi: Użyto druku z porządku wewnętrznego postępowania dyscyplinarnego Policji (art. 135k U.O.P.), a nie właściwego trybu K.P.K./K.P.W. dla zawiadomienia o przestępstwie. Odręczne, chaotyczne dopiski zamiast precyzyjnej podstawy prawnej i wyliczenia załączników. Ponownie ta sama nieprawdziwa teza: „Allegro ma obowiązek wypłacić środki pieniężne”.

Wniosek jest oczywiście jeden: użyto nie tego formularza, co zdradza osobę nie znającą procedur policyjnych.

Granice zaufania, granice fantazji – podsumowanie

Ta historia zaczęła się od śmierdzących kosmetyków, przeszła przez puste paczki otwierane wyłącznie w samochodzie, a skończyła na „policyjnych” dokumentach, które bardziej przypominały teatr jednego aktora niż pisma urzędowe. Po drodze zobaczyliśmy wszystko, co

w e-commerce najciekawsze i najtrudniejsze naraz: jak łatwo ochrona kupującego może stać się pokusą i jak bardzo Allegro Ochrona Kupujących musi łączyć empatię z twardą weryfikacją, by chronić uczciwą większość.

Operacyjnie ten case pokazał trzy rzeczy.

Po pierwsze: eskalacja, od „reklamacji kreatywnych” do fałszywek, bywa standardowym torem nadużyć.

Po drugie: dowody wygrywają z deklaracjami; gdy zdjęcie „oszpecenia” żyje w sieci od lat, a „odmowy policji” mają błędne właściwości i podpisy, narracja sama się sypie.

Po trzecie: współpraca z przewoźnikami i Policją nie jest dodatkiem, tylko częścią mechanizmu bezpieczeństwa i dzięki niej AOK pozostaje tarczą, a nie skarbonką bez dna.

A na deser finał z gatunku komedii omyłek. Zapytana przez dzielnicowego, dlaczego składała wnioski o rekompensatę, zainteresowana odparła bez wahania: „ktoś włamał się na moje konto; ja niczego nie składałam”. Klasyk. Gdyby włamywacze naprawdę mieli czas, by po włamaniu hurtowo zamawiać kremy, chusteczki i kurkumę, a potem jeszcze produkować „pisma” z pieczętkami, musielibyśmy rozważyć model subskrypcyjny dla cyberprzestępców. Na szczęście logi, adresy dostaw i reszta faktów mają jedną wspólną cechę: nie poczucie humoru, tylko pamięć.

„Klienci z zasady są uczciwi” – w jednym zdaniu tak możemy ujednolicić kategoryzację. Ci, którzy poruszają się pod prąd, nazwijmy ich „testerami”, są w zdecydowanej mniejszości. Nieoceniony jest ich wkład w budowanie coraz silniejszych trendów przewencyjnych, odzwierciedlonych w monitoringach, alertach czy im podobnych. Musimy też pamiętać o tym, że na końcu każdej historii znajduje się człowiek.



UCZELNIA PAŃSTWOWA
im. Jana Grodka w Sanoku



ZWALCZANIE PRZESTĘPCZOŚCI INTERNETOWEJ
SANOK 2026