IES

Informatyka sądowa

Badanie dowodów cyfrowych

mgr inż. Robert Radziszewski

Pracownia Informatyki Sądowej

12 422 87 55

rradziszewski@ies.gov.pl

IES

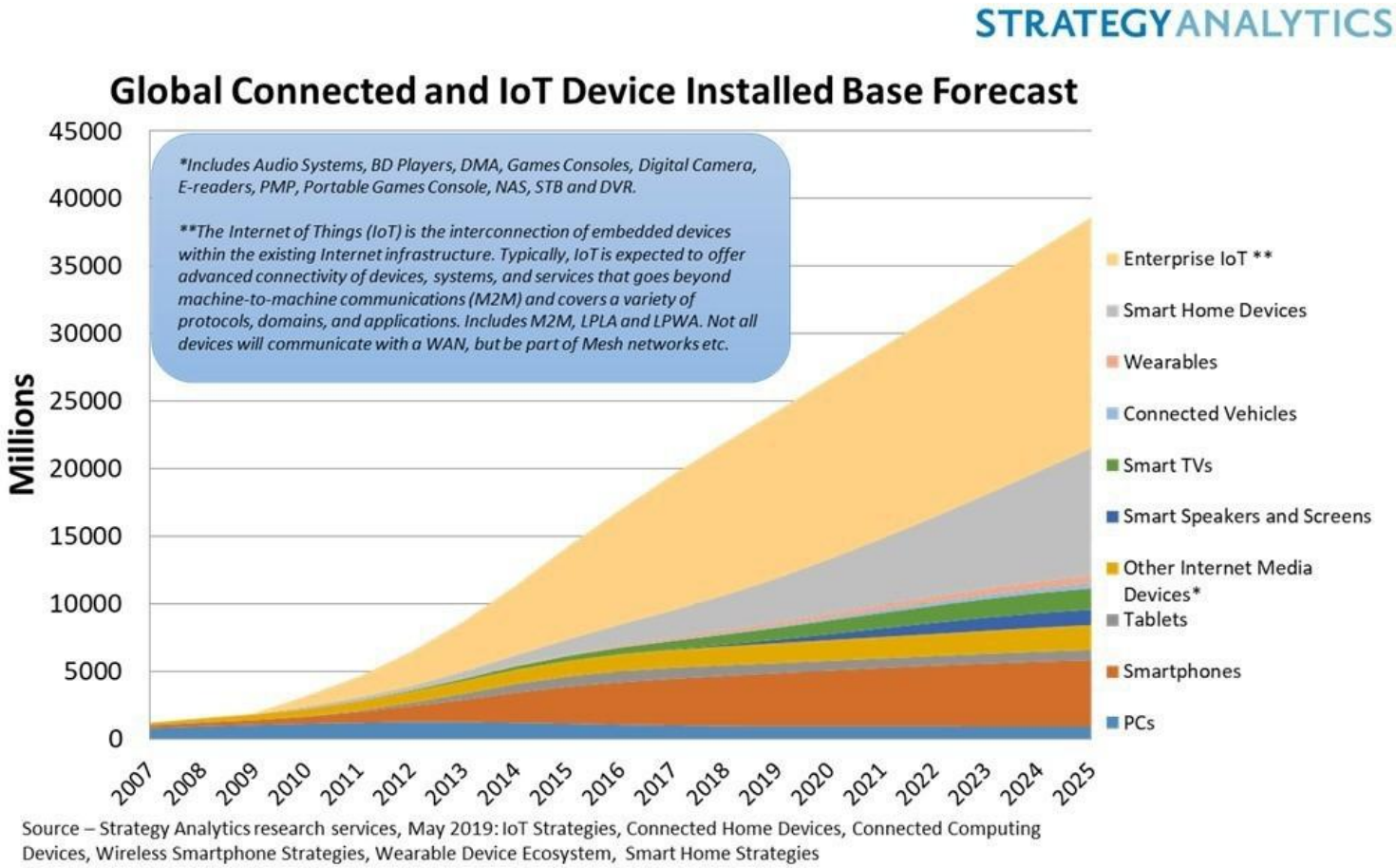
Wstęp

- Ilość danych w Internecie w 2020 roku około 40 – 64 ZB, szacunek w 2025 (prognozy IDC) to 180 ZB.
  (1 ZB = 1 000 000 000 TB)
- Dyski twarde:
  - 1956 - IBM 350: 5 MB
  - 2025 – WD: 24 TB i 40 TB
- Smartfony:
  - 2007 - iPhone 3G: 4-16 GB
  - 2025 – Samsung Galaxy S25 Ultra / iPhone 16 ProMax / Xiaomi 14T Pro: do 1 TB

IES

Wstęp

Ilość urządzeń podłączonych do Internetu



IES

Wstęp

Informatyka sądowa (śledcza) - niekiedy nazywana sądową, (ang. Computer Forensics, CF), to dziedzina informatyki, należąca do gałęzi nauk sądowych, która zajmuje się pozyskiwaniem cyfrowych dowodów przestępstw, oszustw i nadużyć mogących szkodzić interesom firm czy osób prywatnych.

IES

Dowód cyfrowy

• Dowód cyfrowy jest to zbiór informacji przechowywany lub transmitowany w formie binarnej, który może mieć znaczenie dowodowe.

• Dowód cyfrowy można charakteryzować następująco:

  • jest łatwy do modyfikacji

  • ma poszlakowy charakter (wraz z innymi faktami może wskazać sprawcę)

  • wymaga specjalnej wiedzy i środków technicznych do jego zabezpieczenia

  • jego kopia binarna jest równa oryginałowi (wyliczenie sum kontrolnych: MD5, SHA-1, SHA-256)

• Dowody cyfrowe można ogólnie podzielić na dowody rzeczowe (typowe) i dowody uzyskiwane w czasie rzeczywistym (np. dane z podsłuchu)

Dowód cyfrowy

- Ogólne zalecenia:
  - W trakcie zabezpieczania dowodów cyfrowych nie można dopuścić do zmiany zapisanych w nich informacji
  - Każde działanie z dowodem musi być udokumentowane ze wskazaniem osoby i rodzaju przeprowadzonych działań
  - Osoba odpowiednio przeszkolona może dokonać analizy dowodu
  - Analizy należy wykonywać na kopii binarnej dowodu (o ile jest to możliwe)
  - Dowody cyfrowe należy przechowywać w warunkach w jakich zostały znalezione (np. telefon porzucony w zbiorniku wodnym)
  - Urządzenia mobilne należy zabezpieczyć w sposób uniemożliwiający ich przypadkowe włączenie

Dowód cyfrowy

- Rodzaje dowodów cyfrowych:
    - Komputery (np. laptopy, stacjonarne, serwery)
    - Urządzenia specjalizowane (np. rejestratory wideo DVR, urządzenia typu smarthome, urządzenia typu smart speaker/home assistant)
    - Pamięci (np. dyski twarde HDD i SSD, pamięci przenośne, karty pamięci)
    - Urządzenia mobilne (np. telefony, smartfony, tablety, nawigacje satelitarne, smartwatch, smartband)

IES

Dowód cyfrowy

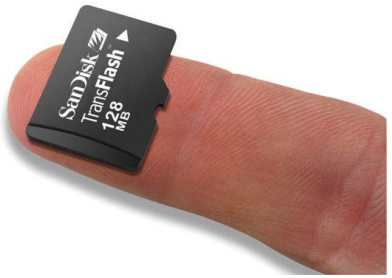
• Dowód cyfrowy, traktowany jako urządzenie fizyczne, może a często jest źródłem dodatkowych śladów np.:

  • ślady genetyczne

  • ślady daktyloskopijne

• Analiza takich dowodów musi uwzględniać kolejność badań w celu uniknięcia zatarcia śladów

• Niektóre badania mogą doprowadzić do uniemożliwienia przeprowadzanie innych badań (np. traktowanie urządzeń odczynnikami chemicznymi).



Komputery, rejestratory wideo, pamięci

• W komputerze i w rejestratorze głównym źródłem informacji jest:

• **Dysk twardy (HDD, SSD)** – zapisana informacja nie jest tracona wraz z utratą zasilania. Wykorzystywany jest do przechowywania danych pochodzących od oprogramowania (w tym systemu operacyjnego) jak i użytkowników.

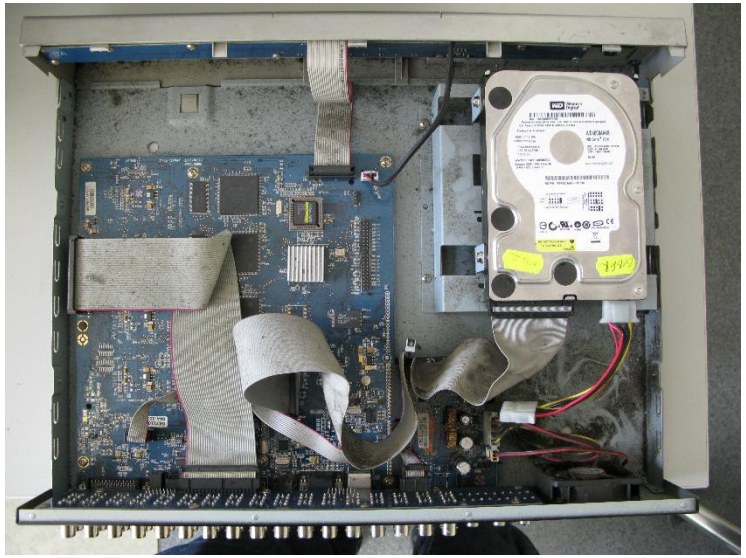
• **Pamięć RAM** – zapisana informacja jest ulotna i zostaje utracona w przypadku zaniku zasilania. Wykorzystywana jest w trakcie pracy komputera i przechowywane są w niej aktualne wykonywane programy oraz wyniki ich pracy.

IES

Komputery, rejestratory wideo, pamięci

- Na nośnikach pamięci znajdują się następujące rodzaje informacji:
    - Informacja zapisana przez oprogramowanie (system operacyjny, itp.)
    - Informacja zapisana przez użytkownika (pliki graficzne, pliki multimedialne, pliki dokumentów, itp.)

- W przypadku rejestratorów wideo zapis na nośniku może odbywać się w sposób ciągły (całodobowo) oraz okresowy (wyzwalany funkcją detekcji ruchu)

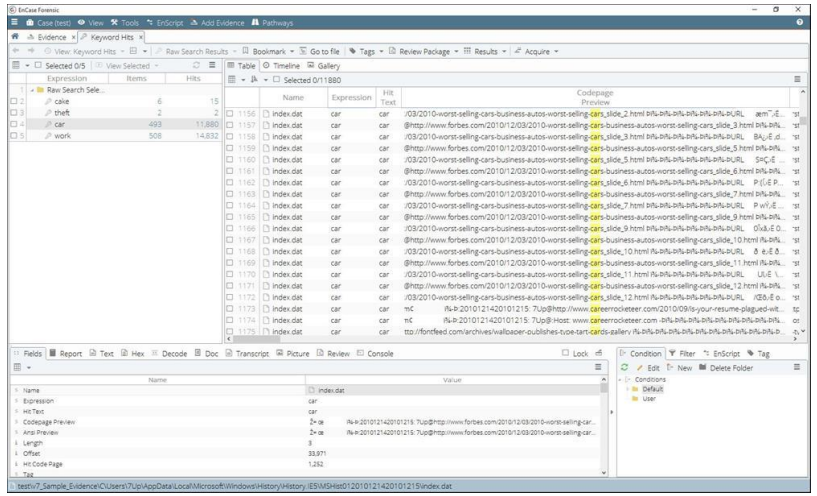


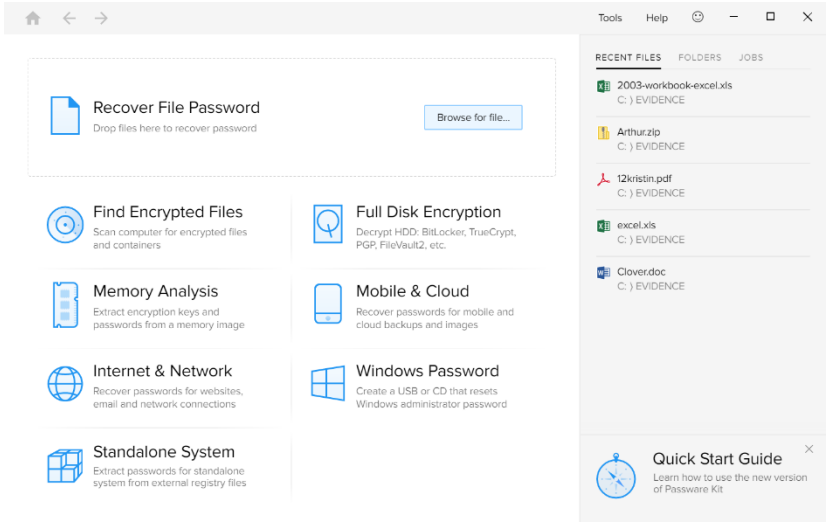
IES

Komputery, rejestratory wideo, pamięci

• Oprogramowanie i urządzenia wspomagające proces analizy pamięci dowodów cyfrowych:

- **Oprogramowanie uniwersalne** (Magnet Axiom, X-Ways Forensics, EnCase Forensics, Forensic Toolkit (FTK), SleuthKit/Autopsy, Cellebrite Inspector)
- **Oprogramowanie specjalizowane** (Passware Kit Forensics – łamanie haseł, Elcomsoft – moduły różnego przeznaczenia, Defraser – odzyskiwanie i rekonstrukcja plików wideo, NirSoft – moduły różnego przeznaczenia, itp.), Cellebrite Digital Collector – obrazowanie komputerów Apple
- **Oprogramowanie i urządzenia tzw. systemy** (PC-3000, DeepSpar Disk Imager – analiza i obrazowanie dysków twardych)
- **Urządzenia specjalizowane** (Tableau – duplikatory, mostki blokujące zapis, adaptery)





Urządzenia mobilne

- Rodzaje urządzeń mobilnych:
  - Telefony GSM
  - Smartfony
  - Tablety
  - Przenośne rejestratory wideo (samochodowe, rowerowe)
  - Smartwatch / smartband (inteligentne zegarki, inteligentne opaski)
  - Przenośne router i modemy (5G, LTE)
  - Nawigacje satelitarne (GNSS: GPS, Galileo, GLONASS, BeiDou, itp..)
  - Dyktafony cyfrowe

Urządzenia mobilne

- W telefonach, smartfonach, tabletach i smartwach-ach źródłem informacji są:
  - Pamięć wewnętrzna – numer IMEI unikalny numer urządzenia nadawany przez producenta
  - Karta SIM – numer ICCID oraz IMSI unikalne numery jednoznacznie ją identyfikujące (w wybranych modelach tabletów i smartwach-y)
  - Karta pamięci – dodatkowa pamięć, zazwyczaj w formacie microSD
- W pozostałych urządzeniach źródłem informacji są:
  - Pamięć wewnętrzna urządzenia

IES

Urządzenia mobilne

- Informacje zapisywane w urządzeniach mobilnych:
  - Książka adresowa, historia połączeń telefonicznych, wiadomości SMS/MMS
  - Pliki graficzne (jpg), pliki wideo (mp4) – wykonane za pomocą wbudowanych aparatów fotograficznych lub z transferu danych
  - Pliki audio (rejestracja z wbudowanego dyktafonu)
  - Informacje o sieciach WiFi z którymi nawiązano łączność
  - Informacje o urządzeniach Bluetooth z którymi nawiązano łączność
  - Informacje o odwiedzanych stronach w sieci Internet
  - Wiadomości poczty elektronicznej
  - Informacje pochodzące z portali społecznościowych i komunikatorów
  - Informacje o punktach gelokalizacyjnych (GNSS: GPS, Galileo, GLONASS, BeiDou, itp.)
  - Informacje o aktywności użytkownika

IES

Urządzenia mobilne

• **eSIM (Embedded SIM)** – wbudowana karta SIM zrealizowana na bazie osobnego chipa umieszczonego na płycie głównej urządzenia w której przechowywane są dane użytkownika, a proces wgrania profilu użytkownika przebiega w systemie OTA (Over-the-Air). Można na nim korzystać z usług wielu operatorów.

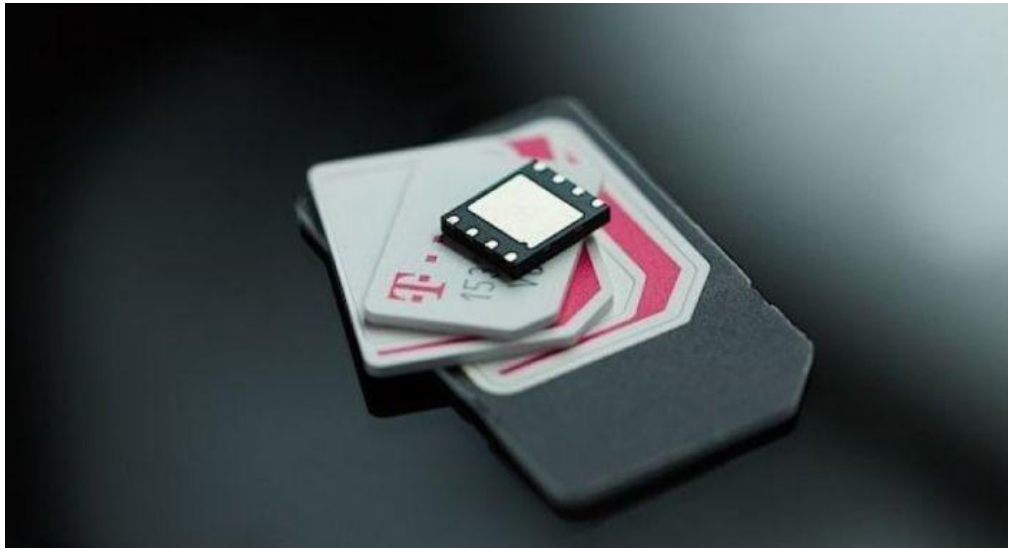
• cechy eSIM:

  • Nie można jej usunąć z urządzenia, integralna część urządzenia

  • Główne hasło blokujące dostęp do eSIM.

  • Większy potencjał wykorzystania (IoT, pojazdy, drony i inne)

• W Polsce wdrożenie technologii u operatorów od 2019 roku - obecnie wspierają wszyscy. Zwiększająca się liczba wspierających urządzeń (np. Google Pixel od 2, iPhone od XS i XR, iPad Pro, Samsung Galaxy od S20 Samsung Gear od S2, Huawei Watch od 2, itp)

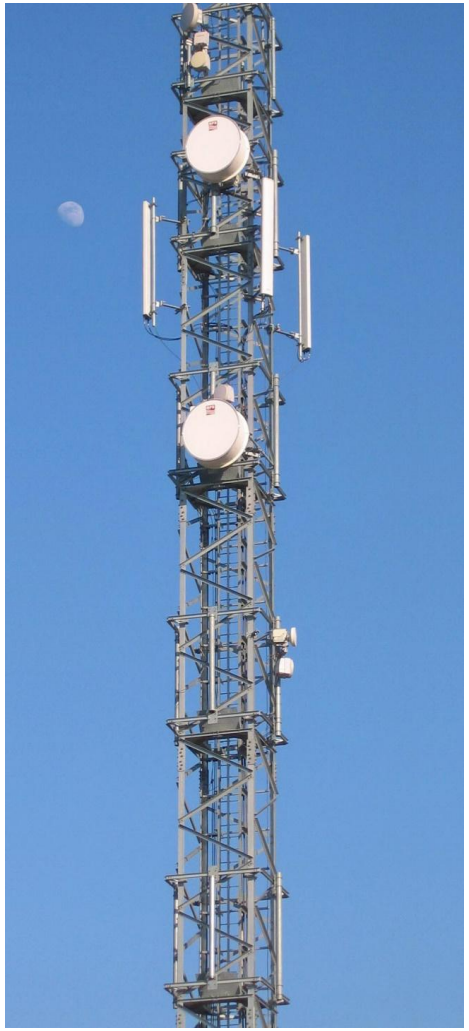


IES

Urządzenia mobilne

- Dane dostępne u operatora sieci komórkowej:
  - Dane powstają w inicjującym połączenie MSC (Mobile Switching Center) i są przesyłane do OMC (Operation and Maintenance Center) - każde połączenie i każda wiadomość
  - Wpis rejestru połączeń (Call Data Record) zawiera zwykle numer MSISDN inicjujący i odbierający połączenie
  - Numery IMEI telefonu inicjującego i odbierającego połączenie
  - Czas trwania połączenia
  - Typ usługi (głosowa, sms, mms, itp.)
  - Identyfikacja pierwszej stacji BTS obsługującej połączenie
  - Numer PUK karty SIM (niezbędny do odblokowania karty z nieznanym kodem PIN)

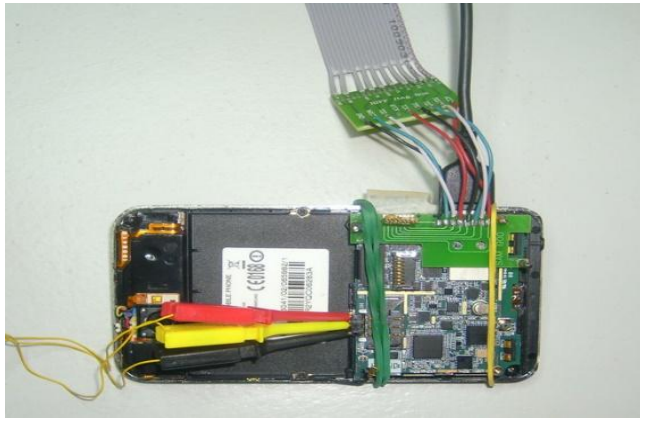
Uwaga: Retencja danych przechowywanych u operatora (12 miesięcy)

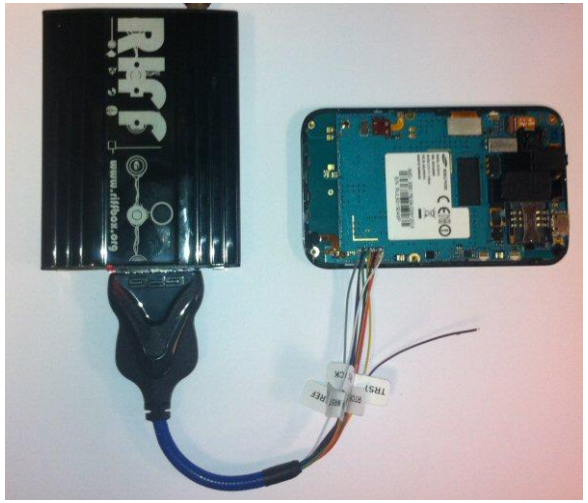


IES

Urządzenia mobilne

- Analiza urządzeń mobilnych (telefonów/smartfonów/tabletów):
  - Odczyt pamięci (interfejs standardowy, JTAG – Joint Test Action Group, Chip-off)
  - Dostęp do pamięci fizyczny
  - Dostęp do pamięci logiczny
  - Interpretacja odczytanych danych:
  - Wykorzystanie gotowych rozwiązań (UFED, XRY, GrayKey, itp.)
  - Manualna analiza w edytorze hexadecymalnym





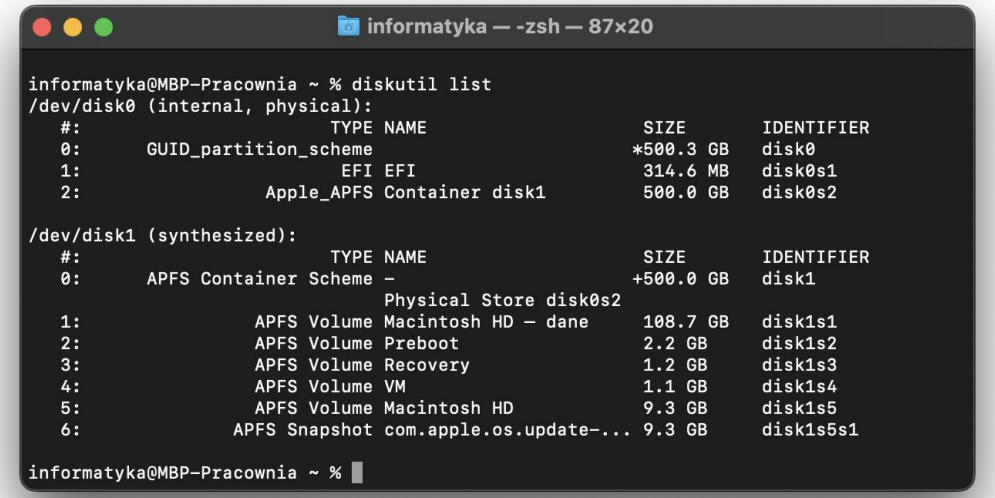
IES

Systemy operacyjne i pliki

- Systemy plikowe najczęściej spotykane w dowodach cyfrowych:
  - NTFS, FAT, EXT, HFS+, APFS, exFAT, itp.
- W systemach plikowych przechowywane są informacje o:
  - Nazwa i typ pliku/katalogu
  - Nazwa właściciela
  - Data i czas utworzenia, modyfikacji
  - Poprzednie wersje plików

- Pliki posiadają własną strukturę w której mogą być umieszczone dodatkowe dane wynikające ze specyfiki pliku oraz programu w którym zostały utworzone

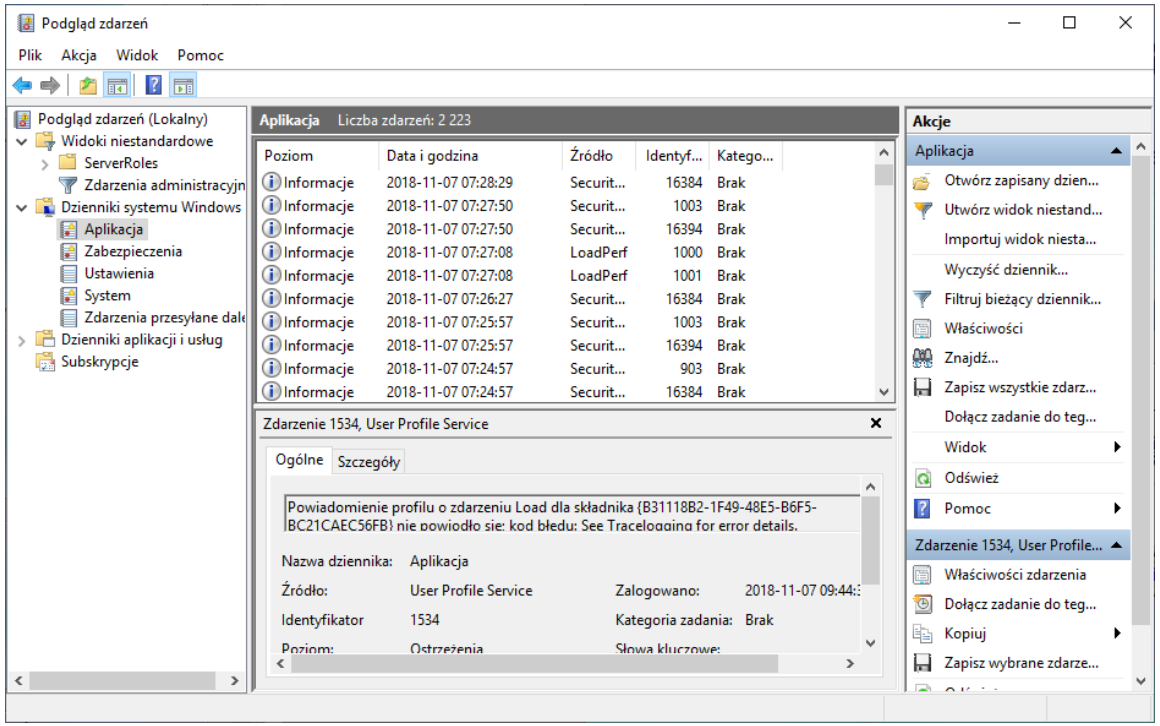
Name	Type	Path	Size
Start sectors		\	1,0 MB
Partition 1	NTFS	\	100 MB
Partition 2 (C:)	NTFS	\	246 GB
Partition 3 (D:)	NTFS	\	686 GB
Partition gap		\	225 KB
Unpartitionable space		\	2,5 MB



Systemy operacyjne i pliki

• Systemy operacyjne zachowują dane konfiguracyjne w rejestrze systemowym (Windows) lub w plikach konfiguracyjnych (Linux - /etc) oraz dzienniku systemowym (Windows) lub też w plikach logów (Linux - /var/log).

- Historia zdarzeń
- Użytkownicy i hasła
- Podłączane dyski
- Podłączane nośniki USB
- Informacje o sieciach (np. WiFi)

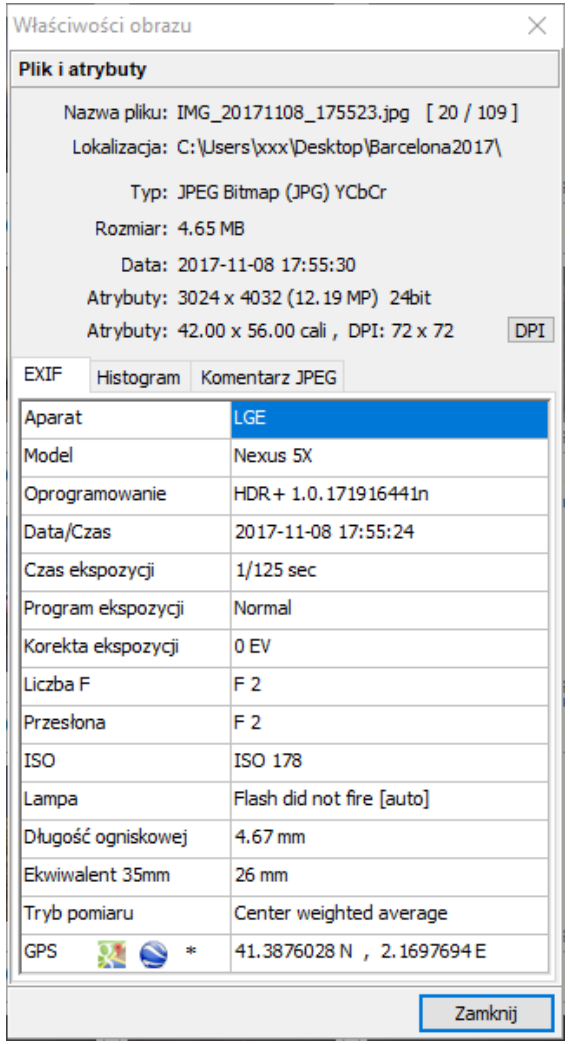


• W programach zainstalowanych w systemach operacyjnych przechowywane są informacje:

- hasła użytkowników (Internet)
- korespondencja
- historia (Internet)

Systemy operacyjne i pliki

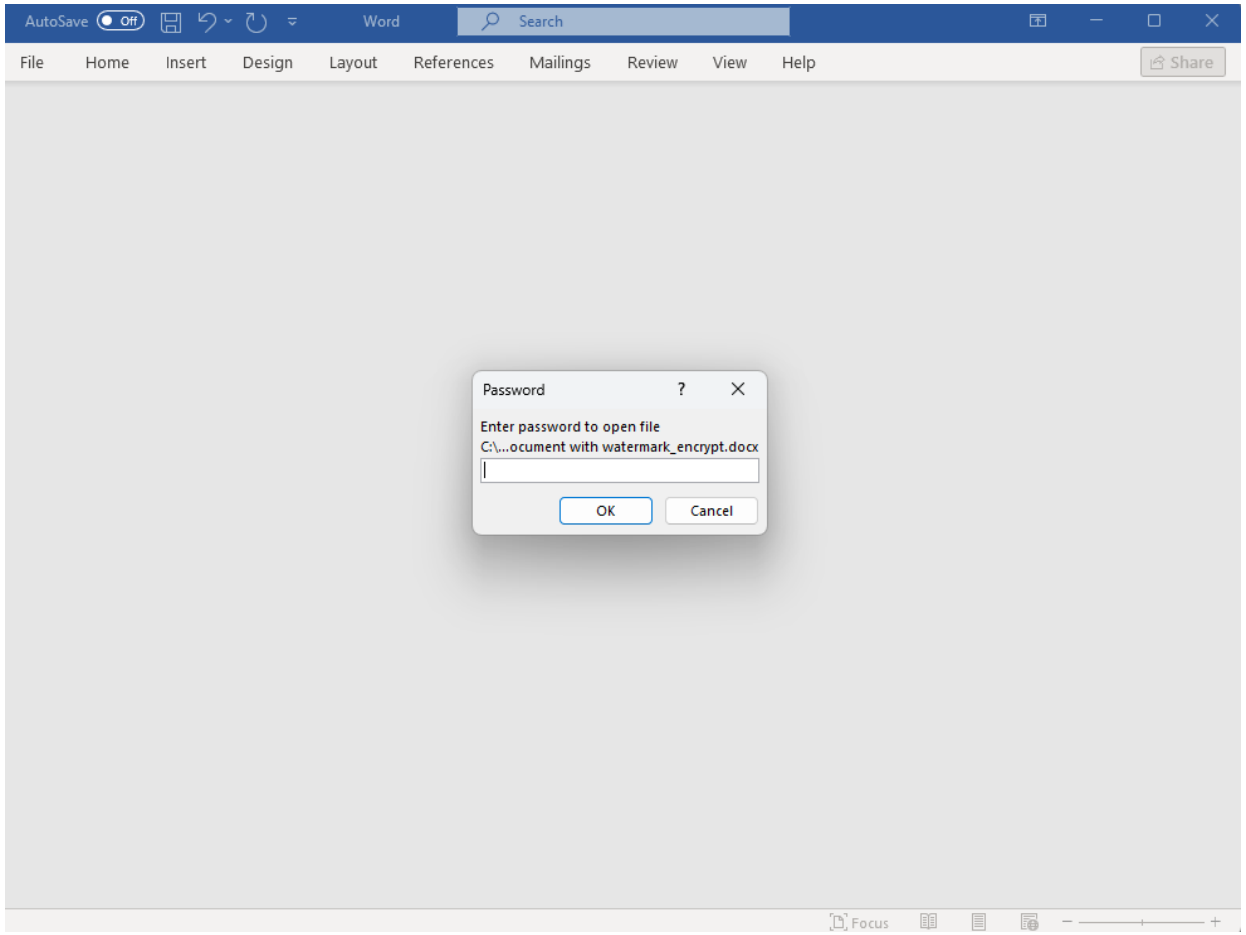
- W plikach mogą być zapisane dodatkowe dane:
  - Pliki dokumentów (MS Word, MS Excel) – temat, tytuł, autor, data/czas (utworzenia, modyfikacji, ostatniego używania, wydruku, numer wersji, itp.)
  - Pliki audio – nazwa, tytuł, wykonawca, autor, czas trwania, informacja o urządzeniu rejestrującym
  - Pliki wideo – rozdzielczość, ilość klatek na sekundę, jakość
  - Pliki graficzne – rozdzielczość, data i czas utworzenia, model aparatu



Systemy operacyjne i pliki

- Szyfrowanie w programie w którym plik został utworzony (MS Word, Open Office/Libre Office, Adobe Reader, Winrar)

- MS Office obecnie szyfrowanie AES-256 bit (w starszych wersjach AES-128 lub szyfrowanie od producenta)
- Adobe Reader obecnie szyfrowanie AES-256 bit (w starszych wersjach AES-128 lub RC4 128 bit)

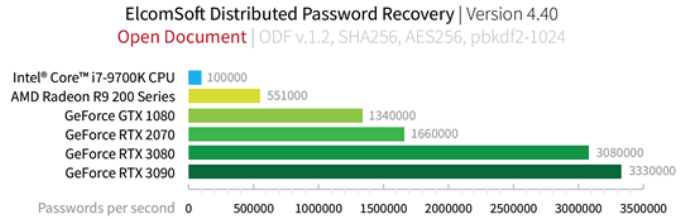


Systemy operacyjne i pliki

Odszyfrowanie plików z wykorzystaniem oprogramowania:

- Passware Forensic Kit
- Elcomsoft Distributed Password Recovery
- DocRecrypt (Microsoft)
- John the Ripper
- Hashcat

Elcomsoft Distributed Password Recovery. Open Office. ODF v.1.2



File Type	Encryption	CPU Speed i7-9700F	NVIDIA Speed GeForce RTX 4070Ti	AMD Speed Radeon RX 6900 XT
MS Office 2013+	AES-256	78	28,557	23,883
RAR 5.x	AES-256	98	114,597	117,867
macOS / FileVault2 / APFS	AES-256	53	65,588	65,392
Apple iTunes Backup / iOS 10.x+	AES-256	<1	372	361
MS Windows / BitLocker	BitLocker	7	3,947	3,623

(passwords/second)

- PDF 1.1 - 1.3 (Acrobat 2 - 4)
- PDF 1.1 - 1.3 (Acrobat 2 - 4), collider #1
- PDF 1.1 - 1.3 (Acrobat 2 - 4), collider #2
- PDF 1.4 - 1.6 (Acrobat 5 - 8)
- PDF 1.4 - 1.6 (Acrobat 5 - 8) - user and owner pass
- PDF 1.7 Level 3 (Acrobat 9)
- PDF 1.7 Level 8 (Acrobat 10 - 11)
- MS Office 2007
- MS Office 2010
- MS Office 2013
- MS Office 2016 - SheetProtection
- MS Office <= 2003 $0/$1, MD5 + RC4
- MS Office <= 2003 $0/$1, MD5 + RC4, collider #1
- MS Office <= 2003 $0/$1, MD5 + RC4, collider #2
- MS Office <= 2003 $3, SHA1 + RC4, collider #1
- MS Office <= 2003 $3, SHA1 + RC4, collider #2
- MS Office <= 2003 $3/$4, SHA1 + RC4
- Open Document Format (ODF) 1.2 (SHA-256, AES)
- Open Document Format (ODF) 1.1 (SHA-1, Blowfish)

Podpis cyfrowy

Podpis cyfrowy – matematyczny sposób weryfikacji autentyczności dokumentów i wiadomości elektronicznych. Prawidłowy podpis oznacza, że wiadomość pochodzi od właściwego nadawcy, który nie może zaprzeczyć, że została wysłana, i że wiadomość nie została zmieniona podczas transmisji.

Podpis cyfrowy może być certyfikowany lub nie, np. graficzny wzór podpisu umieszczony w pliku.

W Polsce:

Ustawa z dnia 5.09.2016 r. o usługach zaufania oraz identyfikacji elektronicznej

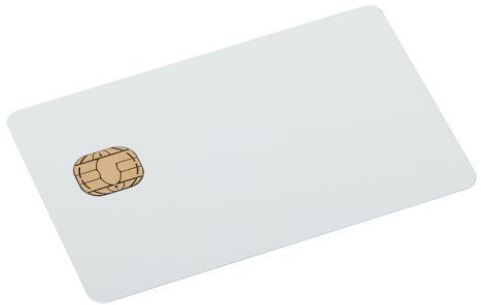
EU akt:

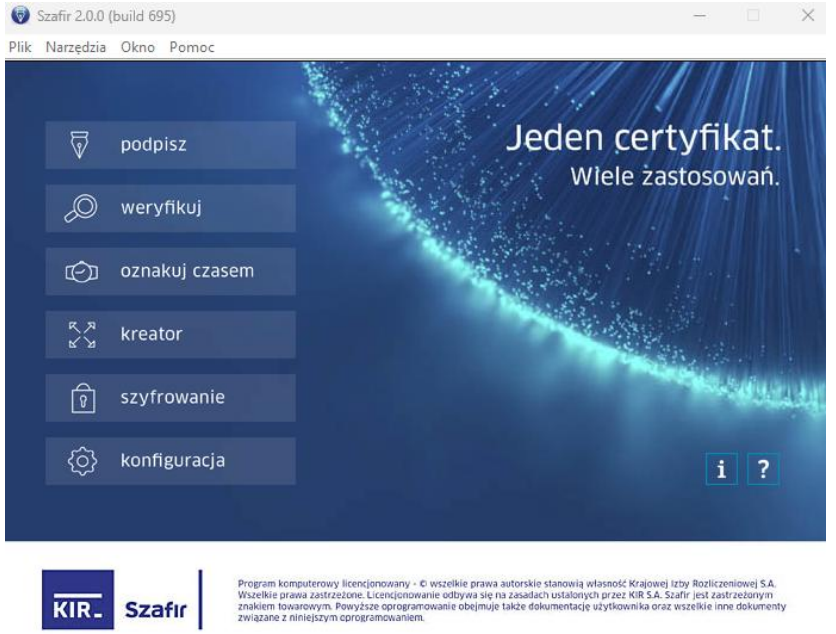
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910

Podpis cyfrowy

Podpis cyfrowy – można zapisać na nośniku typu U2F (np. Yubico), karcie kryptograficznej (HSM) lub specjalnym oprogramowaniu.

Podpis cyfrowy – można zapisać w usługach w chmurze dostępnych u Dostawców Usług Zaufania (typ autoryzacji co najmniej 2FA)

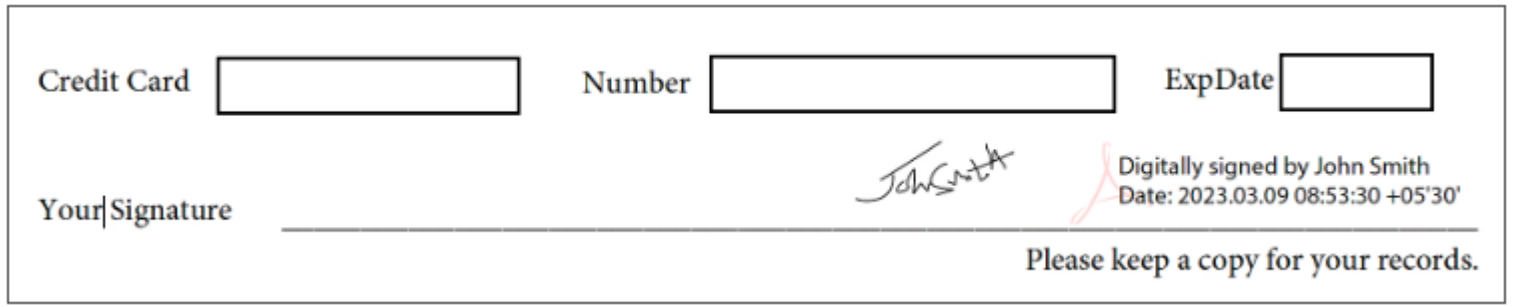




Podpis cyfrowy

Podpis cyfrowy można dodać w popularnych programach, takich jak MS Word i Adobe Reader.

W programie MS Word dodanie pliku powoduje zwiększenie jego rozmiaru (zawiera treść i dane podpisu) i zmianę rozszerzenia na **xades**, np. **paper.doc.xades**.



Source: https://helpx.adobe.com/pl/acrobat/using/certificate-based-signatures.html

IES

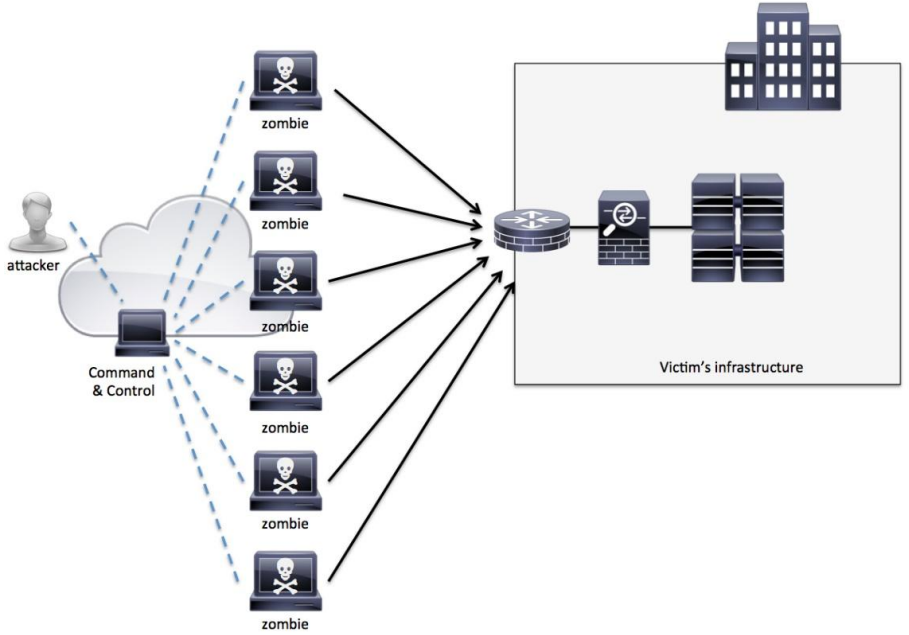
Sieci komputerowe

- Rodzaje cyberataków:
  - **Hacking** – nieautoryzowany dostęp do komputera lub zasobów sieciowych
  - **Phishing** – fałszywe wiadomości mające na celu skłonić odbiorcę do podania poufny danych (np. strona www, email).
  - **Wymuszenia internetowe** (np. Ransomware) – przejęcie kontroli nad systemem ofiary i oddanie kontroli w zamian za korzyść materialną (crypto-locker)
  - Atak na firmę A.P. Moeller-Maersk i Rosneft (WannaCry/Petya - 2018 r.)
  - Atak na infrastrukturę Ukrainy (WannaCry/Petya - 2018 r.)
  - Atak na MPK Kraków (RaaS – 3.12.2024 r.)
  - Atak na firmę EuroCert (ransomware – 12.01.2025 r.)

IES

Sieci komputerowe

- Rodzaje cyberataków:
  - **Kradzież tożsamości** – przejęcie identyfikatorów użytkownika sieci
  - **Blokowanie zasobów sieciowych** (np. DDoS) – zablokowanie dostępu do zasobów poprzez wysyłanie bardzo dużej ilości danych (pakietów) w bardzo krótkim czasie (komputery „zombie").
    - Atak DDoS na serwery home.pl (24.09.2018 r.)



home.pl
24 września ·

Szanowni Państwo,

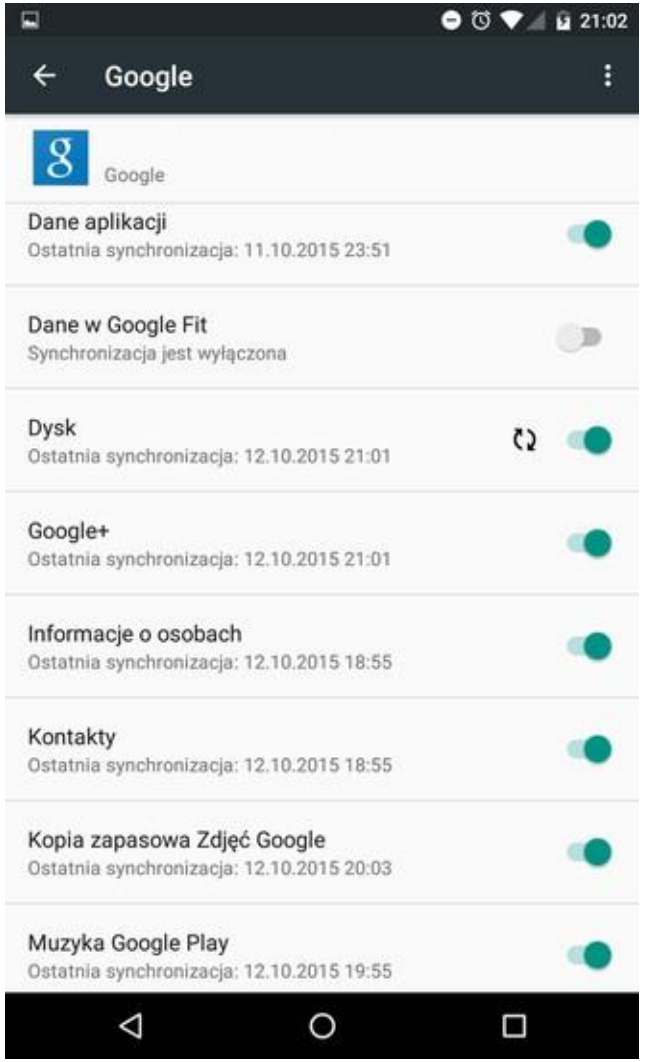
Niedostępność usług home.pl w dniu 24 września 2018 roku związana była z przeprowadzonym przez nieznanych sprawców atakiem DDoS (https://pomoc.home.pl/baza-wiedzy/co-to-jest-atak-ddos) na naszą firmę.

Sieci komputerowe

- Przechowywanie danych w „chmurach”
  - Przechowywanie plików użytkownika (zdjęcia, filmy, kopie zapasowe)
  - Przetwarzanie danych i obliczeń (moc obliczeniowa)
  - Współdzielenie danych z innymi użytkownikami
  - Gromadzenie danych przez firmy prywatne
    - https://myactivity.google.com
    - https://privacy.apple.com

- Najczęściej zasoby chmury wykorzystywane są do synchronizacji danych pomiędzy urządzeniami np. smartfony, tablety, laptopy.
- Synchronizowane dane mogą znajdować się w części lub całości w pamięci kilku urządzeń.

- Problematyka dostępu do danych zapisanych w chmurze
  - Techniczny (ciągły dostęp do danych, lokalizacja)
  - Prawny (RODO, Prawo Telekomunikacyjne)



IES

Inne źródła cyfrowych danych

- Źródło dowodów cyfrowych:
  - **Internet rzeczy (Internet of Things)** – grupa urządzeń, które mogą samodzielnie komunikować się np. lodówka, telewizor, pralka, odkurzacz itp.
  - **Inteligentny dom (Smart Home)** – grupa urządzeń umożliwiających automatyczne zarządzanie budynkiem (rejestratory, czujniki, kamery, zamki, itp.).
  - **Inteligentne głośniki i asystenci domowi (smart speaker and home assistant)** – grupa urządzeń połączona z siecią Internet realizująca usługę asystenta głosowego (Google Home, Amazon Alexa, Apple HomePod).

IES

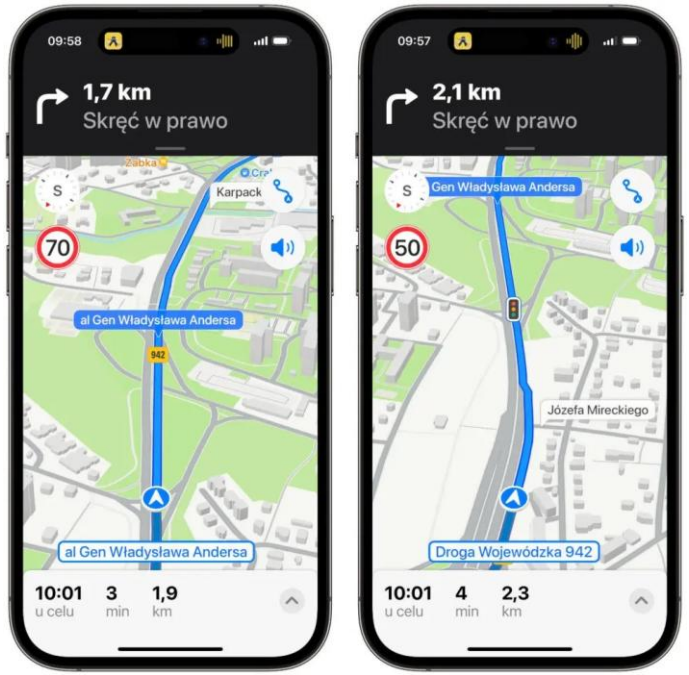
Inne źródła cyfrowych danych

- Źródło dowodów cyfrowych:
  - **Wideorejestratory samochodowe**
    - Zapis strumienia wideo, audio, GNSS
    - Zapis na kartach pamięci
  - **Autonomiczne samochody/pojazdy (self-driving car)**
    - Zapis z komputera pokładowego
    - Zapis z czujników
  - **Drony**
    - Zapis parametrów lotu (GNSS, itp.) wideo i audio
    - Zapis na kartach pamięci
  - **Inteligentne pierścienie (smart rings)**
    - Monitorowanie stanu zdrowia (np. tętno, temperatura ciała)
    - Monitorowanie aktywności fizycznej, snu
    - Płatności bezdotykowe (NFC)
    - Sterowanie innymi urządzeniami (obsługa urządzeń smart)
    - Wymiana danych (Bluetooth, NFC)

Inne źródła cyfrowych danych

Urządzenia mobilne typu smartfon w trakcie użytkowania zapisują dużą ilość danych w tym diagnostycznych.

- Apple iPhone - zapis punktów lokalizacyjnych i prędkości podczas przemieszczania się urządzenia



Projekt badawczy IES w 2024 roku

(Pracownia Wypadków Drogowych i Pracownia Informatyki Sądowej):

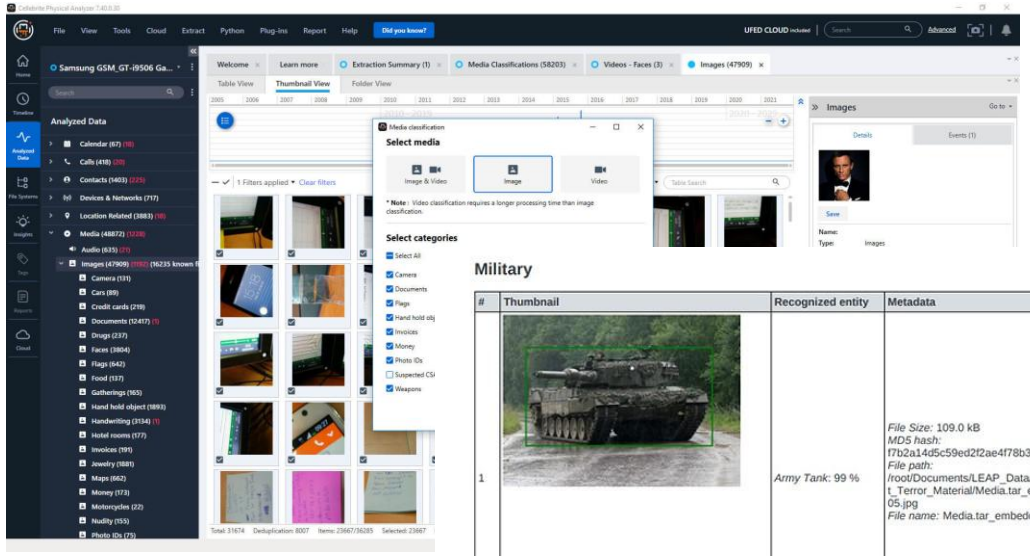
„Walidacja logów prędkości odzyskanych z telefonów Apple iPhone”

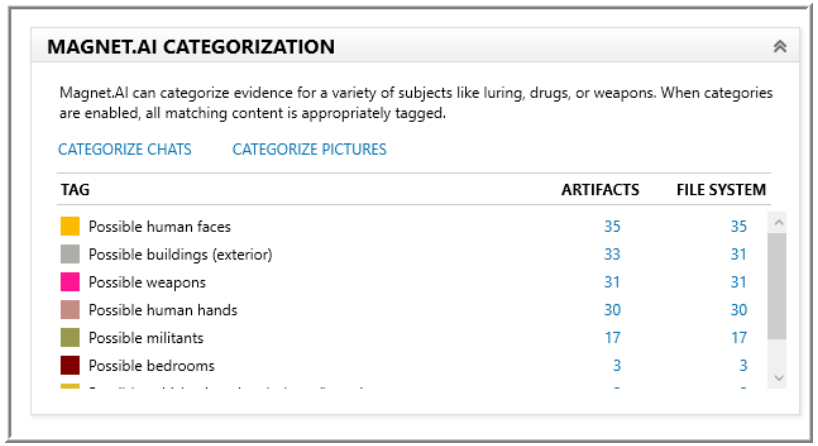
ZALTITUDE	ZCOURSE	ZHORIZONTALACCURACY	ZLATITUDE	ZLONGITUDE	ZSPEED	ZTIMESTAMP
224,180964278989	17,6034155473005	4,85851614683365	50,0851480299901	20,0015924178144	6,64590208927945	02.02.2024 13:50:51
223,992016282864	18,0992169713069	4,8466005020258	50,0850910526277	20,0015665867456	7,00805403097851	02.02.2024 13:50:50
223,873827380128	18,1516705599893	4,84385662091333	50,0850304400307	20,0015354356919	7,25606544748374	02.02.2024 13:50:49
223,706598237157	17,815357186634	4,83878642473236	50,0849686278725	20,0015004778432	7,36595364650648	02.02.2024 13:50:48
223,573206072673	17,6962400105026	4,83796101392408	50,0849069456902	20,0014670664544	7,59955894573616	02.02.2024 13:50:47

Nowe metody analiza cyfrowych danych

Zastosowanie algorytmów w oparciu o techniki głębokiego uczenia maszynowego

- Kategoryzacja zawartości plików (graficzne, wideo, dokumenty, itp.)
- Szacowanie wieku osób w zawartości plików graficznych i wideo (LEAP Tk3.AI)
- Implementacja w specjalistycznym oprogramowaniu (Cellebrite UFED, XRY, Magnet Axiom, itp.)





IES

Sztuczna Inteligencja AI

Sztuczna Inteligencja AI (*ang. Artificial Intelligence*) – system (zbiór zaawansowanych algorytnów), który jest w stanie postrzegać swoje środowisko i podejmować działania, aby zmaksymalizować szansę na pomyśle osiągnięcie swoich celów. System ten jest w stanie interpretować i analizować dane w taki sposób, że uczy się i dostosowuje wraz z upływem czasu.

Generatywna AI – model sztucznej inteligencji zaprojektowany do generowania nowych treści

Popularne modele AI:

- **Chat GPT**– OpenAI, **Copilot**– Microsoft; **Gemini** – Google; **Claude A** – Anthrop\c; **Meta AI**; **DeepSeek** (DeepSeek-R1)
- Bielik, PLLuM
    - Polskie modele generatywnego AI - open source

OpenAI

Gemini

deepseek

Sztuczna Inteligencja AI

Wykorzystanie AI do przestępstw

Deepfake – pierwotnie to technika obróbki obrazu przy użyciu technik sztucznej inteligencji w celu modyfikacji jego treści.

W chwili obecnej terminem **deepfake** określa się wykorzystanie technik sztucznej inteligencji do modyfikacji różnego rodzaju treści, zazwyczaj w celu uzyskania zamierzonego celu niezgodnie z prawem lub przyjętymi normami np.:

- Przestępczość (podszywanie się pod tożsamość ofiary)
- Dezinformacja (polityka)
- Dyskredytacje (kompromitacja, ośmieszanie)

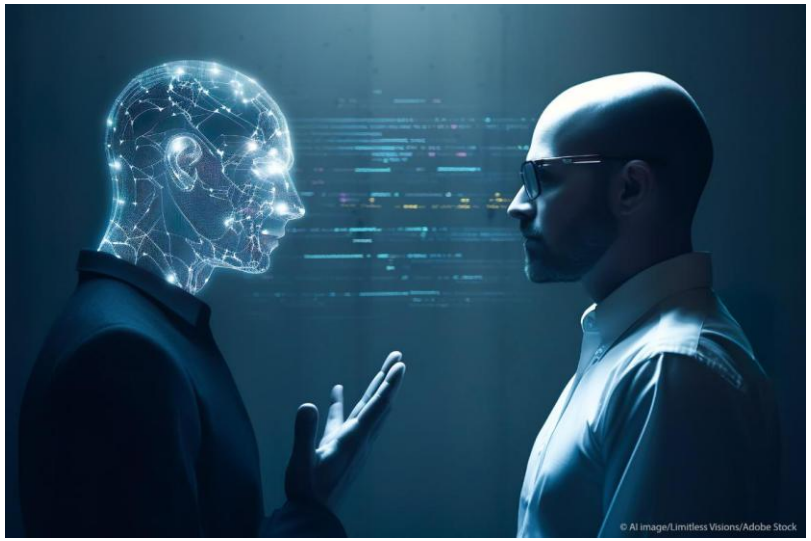
Sztuczna Inteligencja AI

Możliwości analizy materiału typu deepfake

- Wykorzystanie wybranego i dedykowanego modelu AI do wykrywania treści deepfake.

Przykładowe realizacje narzędzi:

- NASK opracowuje narzędzia do wykrywania i rozpoznawani fałszywych materiałów



Ograniczenie negatywnego wpływu treści generowanych przez AI

- Wprowadzenie „znaków wodnych” do treści generowanych przez modele AI
- Ograniczenie dostępu do zasobów danych zgromadzonych w sieci dla modeli AI
- Regulacje prawne dotyczące wykorzystywania AI
    - Dyrektywa UE: **AI Act** (AI Literacy)– pierwsze na świecie kompleksowe przepisy dotyczące AI.
        - 12 lipca 2024 r. przyjęcie uzgodnionego tekstu
        - W Polsce 2 lutego 2025 r. weszły w życie pierwsze przepisy Rozporządzenia o Sztucznej Inteligencji

IES

www.gov.pl/ies

Instytut Ekspertyz Sądowych im. Prof. dra Jana Sehna w Krakowie

Pracownia Informatyki Sądowej

mgr inż. Robert Radziszewski

12 618 58 19

rradziszewski@ies.gov.pl

Instytut Ekspertyz Sądowych

im. Prof. dra Jana Sehna w Krakowie

ul. Westerplatte 9, 31-033 Kraków

12 618 57 00

ies@ies.gov.pl