



**INSTYTUT
EKOLOGII
AKUSTYCZNEJ**

Zabezpieczanie dowodów cyfrowych

Metodologia utrwalania stron internetowych (FireShot Pro + Wayback Machine) oraz własnej dokumentacji (zdjęcia, wideo, audio) z weryfikacją integralności SHA-256

*Poradnik uniwersalny dla społeczności lokalnych, organizacji strażniczych,
grup mieszkańców i aktywistów*

Materiał zrealizowano w ramach projektu „Obywatelska Akademia Ekologii Akustycznej”, finansowanego ze środków Narodowego Instytutu Wolności - Centrum Rozwoju Społeczeństwa Obywatelskiego w ramach Korpusu Solidarności - Rządowego Programu Wspierania i Rozwoju Wolontariatu Systematycznego na lata 2018-2030. Czas realizacji projektu: sierpień 2025 - lipiec 2028. Umowa nr 13/KS/WOW/2025 dotycząca wniosku numer 84854-2. Wysokość dotacji: 456 100,00 zł.



Pole	Wartość
Tytuł	Metodologia zabezpieczania dowodów cyfrowych
Wersja	1.1
Data	19 września 2026
Opracowanie	Klaudia Dąbrowska – specjalistka ds. Komunikacji i edukacji, Instytut Ekologii Akustycznej
Zatwierdzenie	Alan Grinde - Prezes Zarządu, Instytut Ekologii Akustycznej
Licencja	CC BY-SA 4.0 (uznanie autorstwa - na tych samych warunkach)
Kontakt	ekologia.akustyczna@proton.me instytut.ngo

Ważne zastrzeżenie

Niniejszy dokument ma charakter praktyczno-edukacyjny i nie stanowi porady prawnej. Opisane procedury znacząco zwiększają wiarygodność materiału, ale o jego mocy dowodowej zawsze decyduje organ lub sąd, oceniając całokształt okoliczności. W sprawach o dużej wadze (np. proces sądowy, zawiadomienie do prokuratury) rozważ dodatkowo protokół notarialny lub opinię biegłego z zakresu informatyki śledczej.

Spis treści

1. Po co to wszystko? Cel i zasady ogólne
2. Czym jest SHA-256 i co naprawdę udowadnia
3. Przygotowanie stanowiska (jednorazowo)
4. Konfiguracja FireShot Pro - nagłówek i stopka
5. Procedura: zabezpieczenie strony www krok po kroku
6. Wayback Machine - „Save Page Now”
7. Obliczanie i weryfikacja SHA-256 (Windows, macOS, Linux)
8. Własna dokumentacja: zdjęcia, wideo, audio, pomiary
9. Przechowywanie, kopie zapasowe i łańcuch dowodowy
10. Udostępnianie dowodów organom i mediom
11. Najczęstsze błędy

Załącznik A - Karta zabezpieczenia dowodu

Załącznik B - Rejestr sum kontrolnych (manifest)

Załącznik C - Skrypty automatyzujące

Załącznik D - Szybka ściągą (1 strona)

1. Po co to wszystko? Cel i zasady ogólne

Treści w internecie znikają lub zmieniają się bez ostrzeżenia: urząd poprawia komunikat, firma usuwa post, inwestor zmienia opis przedsięwzięcia, ktoś edytuje komentarz. Zwykły zrzut ekranu łatwo podważyć słowami „to mogło być przerobione w programie graficznym”. Celem tej metodologii jest zebranie materiału w taki sposób, aby odpowiedzieć na trzy pytania, które zada każdy sceptyczny urzędnik, sędzia czy dziennikarz:

1. Co dokładnie było widoczne? - pełny zrzut strony w PDF/PNG/JPG.
2. Gdzie i kiedy to było? - adres URL, data i godzina wpisane w nagłówek/stopkę oraz niezależna kopia w publicznym archiwum Wayback Machine z tego samego dnia.
3. Czy od tego czasu nikt tego nie zmienił? - suma kontrolna SHA-256 zapisana w rejestrze w chwili zabezpieczenia i możliwa do sprawdzenia przez każdego.

Pięć zasad ogólnych

- **Zasada podwójnego źródła** każdą ważną stronę zabezpieczamy lokalnie (FireShot) ORAZ publicznie (Wayback Machine). Kopia publiczna jest niezależna od nas, więc nie można nam zarzucić manipulacji.
- **Zasada nienaruszalnego oryginału** plik oryginalny nigdy nie jest edytowany. Adnotacje, kadrowanie, zamazywanie danych - wyłącznie na kopiach roboczych.
- **Zasada natychmiastowego hasza** sumę SHA-256 liczymy od razu po wykonaniu zrzutu/nagrania i przed jakimkolwiek kopiowaniem, wysyłką czy obróbką.
- **Zasada dokumentowania** każdy dowód ma kartę (kto, kiedy, czym, gdzie, dlaczego) - Załącznik A.
- **Zasada 3-2-1** co najmniej 3 kopie, na 2 różnych nośnikach, 1 poza siedzibą/mieszkaniami.

2. Czym jest SHA-256 i co naprawdę udowadnia

SHA-256 to funkcja skrótu (hash), która z dowolnego pliku - zdjęcia, PDF-a, 2-godzinnego nagrania - wylicza unikalny „odcisk palca” o długości 64 znaków szesnastkowych. Zmiana choćby jednego piksela, jednej litery czy jednej sekundy dźwięku daje zupełnie inny wynik. Nie da się w praktyce stworzyć innego pliku o tym samym haszu.

Przykład (skrót jest zawsze tej samej długości, niezależnie od rozmiaru pliku):

Plik: 2026-09-28_073512_www.gmina.pl_Komunikat.pdf
SHA-256:
3A7BD3E2360A3D29EEA436FCFB7E44C735D117C42D1C1835420B6B9942DD4F1B
(wartość przykładowa)

SHA-256 udowadnia	SHA-256 NIE udowadnia
Że plik jest identyczny bit po bicie z plikiem, dla którego wyliczono hasz.	Że treść strony była prawdziwa lub że zrzut nie został przerobiony PRZED policzeniem hasza.
Że nikt nie zmienił pliku od chwili zapisania hasza w rejestrze (jeśli rejestr jest wiarygodny).	Kiedy plik powstał - do tego potrzebny jest niezależny znacznik czasu (Wayback, e-mail, kwalifikowany znacznik czasu).
Że kopia przekazana urzędowi/sądowi jest tą samą, którą zabezpieczyliśmy.	Kto jest autorem pliku - to dokumentuje karta dowodu i łańcuch przekazania.

Jak „zakotwiczyć” hasz w czasie (zalecane)

Sam hasz zapisany u nas na dysku można by teoretycznie podmienić. Dlatego w dniu zabezpieczenia utrwalamy go niezależnie - wybierz jedną lub więcej metod:

- ✓ Wyślij e-mail z listą haszy (manifest) na adres organizacji i do drugiej osoby z zespołu - serwer pocztowy nada niezależną datę.
- ✓ Dołącz manifest do pisma składanego w urzędzie (ePUAP / e-Doręczenia) - urzędowe potwierdzenie przedłożenia z datą.
- ✓ Skorzystaj z kwalifikowanego znacznika czasu (usługa zaufania wg eIDAS, oferowana m.in. przez polskich dostawców podpisu kwalifikowanego) lub bezpłatnego OpenTimestamps - dla spraw najwyższej wagi.
- ✓ Opublikuj sam hasz (nie plik!) np. w komunikacie na stronie organizacji i zarchiwizuj tę stronę w Wayback Machine.

Uwaga: algorytmy MD5 i SHA-1 są przestarzałe (znane kolizje) - używamy wyłącznie SHA-256 (lub SHA-512). Możesz dodatkowo podać MD5 dla kompatybilności ze starszymi systemami, ale nie jako jedyny skrót.

3. Przygotowanie stanowiska (jednorazowo)

- Zsynchronizuj zegar komputera z serwerem czasu (Windows: Ustawienia → Czas i język → „Ustaw czas automatycznie” → „Synchronizuj teraz”; macOS/Linux: automatyczna data i czas). FireShot pobiera datę i godzinę z zegara systemowego - błędny zegar = błędny znacznik w stopce.
- Zanotuj strefę czasową (w Polsce: CET = UTC+1 zimą, CEST = UTC+2 latem). Wayback Machine zapisuje czas w UTC - różnica 1-2 godzin to normalne zjawisko, a nie błąd.
- Zainstaluj FireShot w przeglądarce (Chrome, Firefox, Edge i inne oparte na Chromium) i aktywuj licencję Pro. Na Windows wersja Pro udostępnia dodatkowe okno „Options” z pełną konfiguracją nagłówek, stopek i znaków wodnych (rozdział 4).

- Załóż bezpłatne konto na archive.org - daje dodatkowe opcje „Save Page Now” (zrzut ekranu, zapis linków wychodzących, własne archiwum).
- Przygotuj strukturę folderów (rozdział 9) i plik rejestru (Załącznik B).
- Przygotuj osobny profil przeglądarki „Dowody” - bez rozszerzeń zmieniających wygląd stron (blokey reklam, tryby ciemne, tłumacze), aby zrzut pokazywał stronę tak, jak widzi ją każdy.

Dlaczego w IEA używamy FireShot Pro?

- ✓ Zrzut całej strony (pełna długość, nie tylko widoczny fragment), zaznaczenia lub wszystkich otwartych kart.
- ✓ Zapis do PDF z aktywnymi linkami i przeszukiwalnym tekstem oraz do PNG, JPEG, GIF, BMP.
- ✓ Konfigurowalne nagłówki, stopki i znaki wodne z datą, godziną, tytułem i adresem URL strony - osobno dla PDF i dla obrazów.
- ✓ Tryb wsadowy (lista adresów do automatycznego przechwycenia) - przydatny przy monitoringu wielu stron.
- ✓ Przetwarzanie w 100% lokalne - materiał nie trafia do chmury dostawcy, co ma znaczenie przy danych wrażliwych.
- ✓ W PDF zapisywane są też metadane: tytuł strony, adres źródłowy i czas utworzenia.

4. Konfiguracja FireShot Pro - nagłówek, stopka, nazwy plików

FireShot ma dwa miejsca z ustawieniami: opcje wtyczki w przeglądarce oraz - w wersji Pro na Windows - osobne okno „Options”. Opis poniżej odpowiada rzeczywistym ekranom ustawień (stan: wrzesień 2026). W polskim tłumaczeniu wtyczki część nazw jest niefortunna, np. sekcja „Saving” (zapisywanie) figuruje jako „Oszczędność”.

Gdzie	Jak otworzyć	Co tam ustawiamy
Opcje wtyczki w przeglądarce (strona „Opcje FireShot”)	Ikona FireShot → menu → Opcje	Szablon nazwy pliku, przechwytywanie (opóźnienie, przewijanie), historia, skróty klawiszowe, opcje różne
Okno „Options” FireShot Pro (Windows)	Opcje wtyczki → „Opcje edycji: Kliknij aby przejść do ustawień...” (lub z edytora FireShot Pro)	Capturing (obiekty tekstowe URL i tytułu) oraz Saving → PDF → Header / Footer / Watermark i Saving → Images → Header / Footer / Watermark

Najważniejsza zmiana względem ustawień domyślnych

Domyślny szablon nagłówka PDF to „Page %p %t %u” - zawiera numer strony, tytuł i adres, ale NIE zawiera daty ani godziny wykonania. Dla celów dowodowych trzeba je dopisać (najlepiej w stopce). Nagłówek i stopkę konfigurujemy OSOBNO dla PDF i OSOBNO dla obrazów (PNG/JPG) - to dwie niezależne gałęzie ustawień. Również domyślny szablon nazwy pliku („FireShot Capture %n - %t - [%e]”) nie zawiera daty.

4.1. Pola dostępne w szablonach

Kod	Znaczenie	Kod	Znaczenie
%u	adres URL strony	%H	godzina (0-23)
%t	tytuł strony	%M	minuty
%e	nazwa domeny	%S	sekundy
%y	rok	%U	czas 12-godzinny - NIE używać (niejednoznaczny)
%m	miesiąc (1-12)	%B / %A	nazwa miesiąca / dzień tygodnia
%d	dzień (1-31)	%p	numer strony PDF (tylko nagłówek/stopka PDF)
%w / %h	szerokość / wysokość obrazu	%n	licznik (tylko w nazwie pliku)

Pola najbezpieczniej wstawiać, klikając je na liście pod polem szablonu („click to insert”) - oznaczenia mogą się zmienić w przyszłych wersjach programu.

4.2. Nagłówek i stopka - zalecane szablony

Ścieżka: okno Options → Saving → PDF → Header → zaznacz „Add header” → „Create from text template” → wklej szablon. Następnie Footer (zaznacz „Add footer”), a potem to samo w gałęzi Saving → Images → Header / Footer.

Ustawienie	Szablon do wklejenia
PDF → Header	%t %u
PDF → Footer	Zrzut: %y-%m-%d %H:%M:%S CEST (UTC+2) Zabezpieczył(a): Imię Nazwisko, Organizacja Strona %p
Images → Header	%t %u
Images → Footer	Zrzut: %y-%m-%d %H:%M:%S CEST (UTC+2) Zabezpieczył(a): Imię Nazwisko, Organizacja %wx%h px

Efekt w stopce: „Zrzut: 2026-09-28 07:35:12 CEST (UTC+2) | Zabezpieczył(a): Klaudia Dąbrowska, IEA | Strona 2”.

- **Strefa czasowa:** FireShot nie ma pola strefy czasowej, dlatego wpisujemy ją jako stały tekst. Zmień ją przy przejściu na czas zimowy (ostatnia niedziela października → „CET (UTC+1)”) i letni (ostatnia niedziela marca → „CEST (UTC+2)”). Alternatywa bez pamiętania o zmianie: wpisz „czas lokalny PL”, a strefę notuj w karcie dowodu.
- **Czytelność:** kliknij „Preview and setup style...” - ustaw czcionkę min. 10-11 pt i kontrastowe tło (np. białe). Sprawdź, czy długi adres URL mieści się w całości; jeśli nie, przenieś tytuł %t do stopki, a w nagłówku zostaw sam %u.
- **Placement options:** na podglądzie sprawdź, czy ustawienie „Opacity” nie sprawia, że metryczka jest półprzezroczysta lub niewidoczna, a „Bottom margin” nie przykrywa treści strony. Metryczka ma być w pełni czytelna także na wydruku.
- **Znak wodny (Watermark):** opcjonalny. Jeśli go używasz - umieść na marginesie, nie na treści, żeby nikt nie zarzucił, że coś zasłania. W IEA nie stosujemy znaku wodnego przy zbieraniu materiału dowodowego.

4.3. Capturing - obiekty tekstowe URL i tytułu

W gałęzi Capturing warto zaznaczyć „Add webpage URL as Text object” oraz „Add webpage title as Text object”. Uwaga na istotną różnicę: te obiekty tekstowe pojawiają się w edytorze i są edytowalne (można je przesunąć, zmienić lub usunąć), więc same w sobie nie stanowią zabezpieczenia. Wartość dowodową ma nagłówek i stopka nanoszone automatycznie przy zapisie oraz metadane PDF. Obiekty tekstowe traktuj jako wygodny dodatek przy kopiach roboczych z adnotacjami.

4.4. Szablon nazwy pliku (opcje wtyczki)

Szablon nazwy pliku znajduje się w opcjach wtyczki w przeglądarce: sekcja „Oszczędność” → „Domyślna nazwa szablonu” (w oknie Options widnieje tylko informacja „Filename Template settings relocated”). Zalecany szablon:

```
%y-%m-%d_%H%M%S_%e_%t  
np. 2026-09-28_073512_www.gmina.pl_Komunikat w sprawie farmy wiatrowej.pdf
```

Wariant z licznikiem (wiele zrzutów w tej samej sekundzie, np. tryb wsadowy):
%y-%m-%d_%H%M%S_%e_%n_%t

- Zaznacz „Numer Pada z 3 Zera” - dopełnienie licznika zerami (001, 002...) daje poprawne sortowanie.
- Limit długości nazwy (domyślnie 100 znaków) można zostawić - obetnie się najwyżej końcówka tytułu, a pełne dane są w nagłówku i metadanych PDF.
- Znaki niedozwolone w nazwach plików (np. „/”, „:”) są zamieniane na podkreślniki - to normalne.

4.5. Przechwytywanie i pozostałe opcje wtyczki

Opcja	Zalecenie	Dlaczego
Opóźnienie przed wykonaniem zrzutu	3-5 s (tryb aktywuje się, przytrzymując Alt przy uruchamianiu FireShot)	Strony „doładują” obrazy i komentarze - opóźnienie zmniejsza ryzyko pustych miejsc
Zezwalaj na nieskończone przewijanie	Włączone dla mediów społecznościowych i długich wątków	Pozwala uchwycić całą dyskusję; przy bardzo długich stronach plik bywa ogromny - wtedy zrób kilka zrzutów części
Maksymalny czas na załadowanie strony	Bez zmian (np. 1200 s)	Wystarcza nawet dla wolnych serwisów urzędowych
„Przechwyć wszystkie zakładki” tylko widoczną część	Wyłączone	Chcemy pełnych stron także przy przechwytywaniu wielu kart
Historia (np. 30 dni)	Dowolnie	Historia FireShot to wygoda, nie archiwum - oryginały zawsze przenosimy do folderu 01_ORYGINALY
Automatyczne zgłaszanie błędów	Rozważ wyłączenie na stanowisku „Dowody”	Ostrożność przy materiałach wrażliwych
Powiadom mnie o aktualizacji	Włączone	Wiesz, jakiej wersji używasz - wpisujesz ją do karty dowodu

4.6. Test konfiguracji

- Zrób zrzut dowolnej strony zapisem bezpośrednim („Zapisz jako PDF” / „Zapisz jako obraz”), bez przechodzenia przez edytor.
- Sprawdź na KAŻDEJ stronie PDF: pełny URL, tytuł, datę i godzinę zgodne z zegarem systemowym, numer strony.
- Powtórz test dla PNG/JPG (gałąź Images).
- Otwórz właściwości PDF (Ctrl+D w większości czytników) i sprawdź metadane: tytuł, adres źródłowy, datę utworzenia.
- Zachowaj zrzuty testowe i zrzuty ekranów ustawień jako wzorzec - przydadzą się, gdy ktoś zapyta „jak program był skonfigurowany?”.

5. Procedura: zabezpieczenie strony www krok po kroku

Cała procedura dla jednej strony zajmuje ok. 5-10 minut. Najlepiej wykonywać ją w parach - jedna osoba wykonuje, druga (nawet zdalnie) jest świadkiem i podpisuje kartę.

- Otwórz stronę w profilu „Dowody”. Poczekaj na pełne załadowanie. Zamknij banery cookies (zanotuj, że to zrobiłeś/-aś), ale nie loguj się, jeśli nie jest to konieczne.
- Zrób zrzut CAŁEJ strony w FireShot: „Przechwyć całą stronę” → „Zapisz jako PDF” (dokument główny) - bezpośrednio, bez edytora. Zapisz też wersję PNG (bezstratna) do publikacji i porównań. JPG tylko pomocniczo (kompresja stratna).
- Jeśli istotny jest konkretny fragment (np. komentarz), wykonaj dodatkowo zrzut zaznaczenia - ale zawsze obok zrzutu całej strony, by pokazać kontekst.
- Sprawdź, czy nagłówek i stopka zawierają URL, tytuł, datę i godzinę.
- Natychmiast policz SHA-256 każdego zapisanego pliku (rozdział 7) i wpisz do rejestru (Załącznik B).
- W tej samej sesji zgłoś adres do Wayback Machine - „Save Page Now” (rozdział 6). Skopiuj otrzymany adres archiwalny (web.archive.org/web/RRRRMMDDGGMMSS/...).
- Opcjonalnie: zapisz zrzut całego pulpitu (PrtScn / Win+Shift+S) pokazujący pasek adresu przeglądarki i zegar systemowy - prosty, dodatkowy kontekst.
- Opcjonalnie dla spraw dużej wagi: nagraj ekran (wideo) podczas wchodzenia na stronę - od wpisania adresu po przewinięcie treści. Nagranie również haszujesz.
- Wypełnij kartę zabezpieczenia dowodu (Załącznik A) - wpisz hasze, adres archiwalny i wersję FireShot.
- Wyślij manifest haszy e-mailem na adres organizacji i do drugiej osoby (zakotwiczenie w czasie).
- Przenieś oryginały do folderu „01_ORYGINALY” (tylko do odczytu) i wykonaj kopie zapasowe (rozdział 9).

Media społecznościowe i strony wymagające logowania

Wayback Machine często nie zarchiwizuje treści widocznych tylko po zalogowaniu (np. grupy na Facebooku). Wtedy: (1) wykonaj zrzut FireShot i nagranie ekranu, (2) zanotuj bezpośredni link do posta i nazwę profilu, (3) w wyjątkowo ważnych sprawach rozważ protokół notarialny z przeglądania strony. Pamiętaj o ochronie danych osobowych osób trzecich - w materiałach publikowanych zamazuj dane prywatnych osób (na kopii, nie na oryginale!).

6. Wayback Machine - „Save Page Now”

Internet Archive (web.archive.org) to niezależne, publiczne archiwum internetu. Kopia wykonana przez „Save Page Now” (SPN) jest przechowywana przez podmiot trzeci, otrzymuje znacznik czasu i jest dostępna dla każdego - to najmocniejszy argument przeciwko zarzutom o manipulację.

6.1. Krok po kroku

- Wejdź na web.archive.org/save (lub na stronę główną Wayback Machine - formularz „Save Page Now”). Zaloguj się na konto archive.org.
- Wklej pełny adres URL strony (ten sam, który widnieje w nagłówku zrzutu FireShot).
- Zaznacz opcje: „Save screenshot” (archiwum wykona własny zrzut), „Save outlinks” - jeśli strona zawiera linki do istotnych załączników, np. PDF-ów z decyzjami; „Save error pages” - jeśli chcesz udokumentować, że strona zniknęła (błąd 404/500). Opcjonalnie „Save also in my web archive”.
- Kliknij „SAVE PAGE” i poczekaj na zakończenie. Skopiuj adres archiwalny w formacie: <https://web.archive.org/web/20260928053512/https://www.przyklad.pl/strona>
- Otwórz adres archiwalny i sprawdź, czy treść jest widoczna. Zrób zrzut FireShot także tej wersji archiwalnej (z metryczką) - dokumentuje to skuteczność archiwizacji.
- Wpisz adres archiwalny do karty dowodu i rejestru.

6.2. Jak czytać znacznik czasu

Liczba w adresie archiwalnym to data i godzina w formacie RRRRMMDDGGMMSS w czasie UTC. Przykład: 20260928053512 = 28.09.2026, 05:35:12 UTC = 07:35:12 czasu polskiego (CEST). Zgodność tej godziny z godziną w stopce FireShot (z dokładnością do kilku minut) wzajemnie potwierdza oba dowody.

6.3. Ograniczenia i dobre praktyki

- SPN bez opcji „outlinks” zapisuje wyłącznie wskazaną stronę (z obrazami i CSS), a nie cały serwis - ważne podstrony i załączniki zgłaszaj osobno lub z opcją „Save outlinks”.
- Załączniki PDF (np. decyzje, raporty OOS) zgłaszaj bezpośrednim linkiem do pliku - archiwum zapisze sam dokument.
- Niektóre serwisy blokują archiwizację, a treści ładowane dynamicznie mogą się nie wyświetlić - zawsze sprawdź wynik.
- Archiwizuj regularnie strony, które mogą się zmieniać (np. co tydzień w trakcie konsultacji społecznych) - powstaje oś czasu zmian.
- Zgłoszenia wielu adresów można zautomatyzować (API SPN2 dla zalogowanych, rozszerzenie przeglądarki Wayback Machine) - patrz Załącznik C.

7. Obliczanie i weryfikacja SHA-256

Do liczenia haszy nie potrzeba dodatkowych programów - narzędzia są wbudowane w systemy operacyjne. Wynik jest identyczny niezależnie od systemu (wielkość liter nie ma znaczenia).

System	Polecenie
Windows - PowerShell	Get-FileHash "C:\Dowody\plik.pdf" -Algorithm SHA256
Windows - Wiersz poleceń	certutil -hashfile "C:\Dowody\plik.pdf" SHA256
macOS - Terminal	shasum -a 256 /sciezka/plik.pdf
Linux - Terminal	sha256sum /sciezka/plik.pdf
Windows - graficznie	7-Zip: prawy klik na pliku → CRC SHA → SHA-256

7.1. Hasz całego folderu (manifest)

Przy wielu plikach tworzymy jeden plik-manifest z haszami wszystkich plików. Manifest też haszujemy i wysyłamy e-mailem.

```
# Windows PowerShell - manifest folderu sprawy
Get-ChildItem "C:\Dowody\2026-09_Sprawa\01_ORIGINALY" -Recurse -File |
  Get-FileHash -Algorithm SHA256 |
  Select-Object Hash, Path |
  Export-Csv "C:\Dowody\2026-09_Sprawa\SHA256_manifest.csv" -NoTypeInfoInformation -
  Encoding UTF8
```

```
# Linux / macOS - manifest i późniejsza weryfikacja
cd 01_ORIGINALY
find . -type f -exec sha256sum {} \; > ../SHA256SUMS.txt    # macOS: shasum -a 256
sha256sum -c ../SHA256SUMS.txt                            # każdy plik: OK / FAILED
```

7.2. Weryfikacja przez odbiorcę

Osoba otrzymująca plik (urzędnik, prawnik, dziennikarz) liczy hasz u siebie tym samym poleceniem i porównuje z wartością z karty dowodu. Identyczny wynik = plik nie został zmieniony. W piśmie przewodnim warto zamieścić krótką instrukcję (rozdział 10).

8. Własna dokumentacja: zdjęcia, wideo, audio, pomiary

Te same zasady stosujemy do materiałów, które wytwarzamy sami w terenie: fotografii, nagrań wideo, nagrań dźwiękowych, plików z mierników poziomu dźwięku, notatek i protokołów.

8.1. Przed wyjściem w teren

- Ustaw w aparacie, telefonie, rejestratorze i mierniku poprawną datę, godzinę i strefę czasową. Na początku sesji sfotografuj ekran zegara referencyjnego (np. time.is w telefonie) - to „kalibracja czasu”.
- Włącz geotagowanie (GPS) w aparacie/telefonie, jeśli lokalizacja ma znaczenie.
- Nagrywaj w najwyższej rozsądnej jakości i formatach możliwie bezstratnych: zdjęcia RAW + JPG, audio WAV/BWF (np. 24 bit / 48 kHz), wideo w natywnym formacie urządzenia.
- Przygotuj puste, sformatowane karty pamięci.

8.2. W trakcie dokumentacji

- Na początku nagrania wideo/audio wypowiedz „slate”: data, godzina, miejsce, osoba, cel. Np. „28 września 2026, 22:10, ul. Leśna 5, pomiar hałasu nocnego, nagrywa Klaudia Dąbrowska”.
- Pokaż kontekst: szerokie ujęcie miejsca, tablica z adresem, źródło hałasu, a dopiero potem zbliżenia.
- Przy pomiarach akustycznych fotografuj ekran miernika i jego ustawienia (charakterystyka A/C, stała czasowa, kalibracja) oraz zapisz plik z miernika.
- Nie kasuj „nieudanych” ujęć - ciągłość numeracji plików (DSC_0101, 0102, 0103...) to argument, że nic nie usunięto.

8.3. Po powrocie - procedura „zrzutu karty”

4. Skopiuj CAŁĄ zawartość karty pamięci (bez selekcji, bez zmiany nazw) do folderu 01_ORYGINALY/RRRR-MM-DD_urządzenie.
5. Natychmiast wygeneruj manifest SHA-256 dla tego folderu (rozdział 7.1).
6. Porównaj hasze kilku plików na karcie i na dysku - potwierdzenie wiernego kopiowania.
7. Ustaw folder jako tylko do odczytu (Windows: Właściwości → „Tylko do odczytu”; Linux/macOS: chmod -R a-w).
8. Wyślij manifest e-mailem (zakotwiczenie w czasie), wykonaj kopie zapasowe.
9. Pracuj wyłącznie na kopiach w folderze 03_ROBOCZE (montaż, kadrowanie, normalizacja audio, anonimizacja). Każdy plik wynikowy przeznaczony do przekazania też haszujesz - a w karcie opisujesz, z jakiego oryginału powstał i jak został przetworzony.

8.4. Metadane - zachowaj i udokumentuj

Metadane (EXIF w zdjęciach, znaczniki czasu i dane urządzenia w wideo/audio, metadane BWF) są dodatkowym dowodem. Nie usuwaj ich z oryginałów. Do odczytu przydają się bezpłatne narzędzia: ExifTool (zdjęcia i większość formatów) i MediaInfo (wideo/audio). Raport metadanych można zapisać do pliku tekstowego i również zahaszować.

```
exiftool -a -G1 -s 01_ORYGINALY\DSC_0101.NEF > 02_METADANE\DSC_0101_exif.txt
```

Uwaga o komunikatorach i mediach społecznościowych

Wysyłka zdjęcia/wideo przez WhatsApp, Messenger, Facebook itp. zwykle kompresuje plik i usuwa metadane - powstaje NOWY plik z innym haszem. Dowody przekazuj jako oryginalne pliki (dysk w chmurze, pendrive, archiwum ZIP), a do publikacji w mediach społecznościowych używaj kopii roboczych.

Typ materiału	Format oryginału	Co dodatkowo zabezpieczyć
Strona www	PDF (FireShot) + PNG	Adres Wayback, metryczka URL/tytuł/data/godzina, nagranie ekranu (opcjonalnie)
Zdjęcie	RAW + JPG z aparatu/telefonu	EXIF, GPS, ciągłość numeracji
Wideo	Natywny plik z urządzenia (MP4/MOV)	Słate na początku, raport MediaInfo
Audio	WAV/BWF (bezstratny)	Słate, ustawienia rejestratora, kalibracja
Pomiar akustyczny	Plik eksportu z miernika + zdjęcia ekranu	Świadectwo wzorcowania, ustawienia, warunki meteo
Dokumenty/pisma	PDF oryginalny / skan PDF	UPO z ePUAP, data wpływu, hasz
E-mail	Plik .eml (z nagłówkami)	Pełne nagłówki techniczne, załączniki osobno

9. Przechowywanie, kopie zapasowe i łańcuch dowodowy

9.1. Struktura folderów sprawy

```

RRRR-MM_NazwaSprawy/
├── 00_KARTY/          karty zabezpieczenia dowodów (Załącznik A), notatki
├── 01_ORYGINALY/      pliki nietknięte - TYLKO DO ODCZYTU
│   ├── WWW/          zrzuty FireShot (PDF, PNG), nagrania ekranu
│   ├── FOTO/
│   ├── WIDEO/
│   ├── AUDIO/
│   └── POMIARY/
├── 02_METADANE/       raporty EXIF/MediaInfo, adresy Wayback (lista .txt)
├── 03_ROBOCZE/        kopie do edycji, montażu, anonimizacji
├── 04_DO_PRZEKAZANIA/ finalne pakiety dla urzędu/sądu/mediów (+ ich hasze)
├── SHA256_manifest.csv rejestr sum kontrolnych
└── LOG_dostepu.txt    kto, kiedy i po co korzystał z materiałów
  
```

9.2. Zasada 3-2-1 w praktyce

- **Kopia 1** dysk roboczy komputera (folder sprawy).
- **Kopia 2** dysk zewnętrzny lub NAS, podłączany tylko na czas kopiowania (ochrona przed ransomware).
- **Kopia 3** chmura organizacji (np. Dysk Google / OneDrive) z włączoną historią wersji i logowaniem dwuskładnikowym; dla materiałów wrażliwych - archiwum szyfrowane (np. 7-Zip AES-256 lub VeraCrypt).
- **Co 6-12 miesięcy** weryfikacja haszy wszystkich kopii (sha256sum -c lub skrypt C.2) - wykrywa uszkodzenia nośników.
- **Po zakończeniu sprawy** archiwizacja na nośniku długoterminowym, opis w rejestrze, określenie okresu przechowywania.

9.3. Łańcuch dowodowy (chain of custody)

Łańcuch dowodowy to udokumentowana historia każdego pliku: kto go wytworzył, kto miał do niego dostęp, komu i kiedy go przekazano. W praktyce wystarczy prowadzić LOG_dostepu.txt oraz sekcję „Przekazania” w karcie dowodu. Przy każdym przekazaniu podajemy hasz - odbiorca może go od razu sprawdzić.

9.4. Ochrona danych osobowych

Materiały dowodowe często zawierają wizerunki, głosy, numery rejestracyjne czy dane osób trzecich. Dostęp ograniczamy do osób, które go potrzebują; publikujemy wyłącznie zanonimizowane kopie robocze; ustalamy okres przechowywania i usuwamy materiały zbędne. Oryginały nieanonimizowane przekazujemy wyłącznie organom i pełnomocnikom w związku z konkretną sprawą.

10. Udostępnianie dowodów organom i mediom

- Przygotuj pakiet w 04_DO_PRZEKAZANIA: pliki, karty dowodów, manifest SHA-256, lista adresów Wayback.
- Spakuj pakiet do ZIP i policz hasz samego archiwum ZIP.
- W piśmie przewodnim wymień pliki z haszami i adresami archiwalnymi oraz dodaj krótką instrukcję weryfikacji.
- Zachowaj potwierdzenie przekazania (UPO z ePUAP/e-Doręczeń, potwierdzenie nadania, protokół odbioru).

Wzór akapitu do pisma

„Do niniejszego pisma załączam materiał dowodowy w postaci zrzutów stron internetowych wykonanych w dniu 28.09.2026 r. narzędziem FireShot Pro (z automatycznie naniesionym w nagłówku adresem URL i tytułem strony oraz w stopce datą i godziną wykonania) wraz z kopiami tych stron zapisanymi w tym samym dniu w publicznym archiwum Internet Archive (Wayback Machine) pod adresami wskazanymi w wykazie. Integralność każdego pliku można zweryfikować, obliczając jego sumę kontrolną SHA-256 (np. w systemie Windows poleceniem: certutil -hashfile nazwa_pliku SHA256) i porównując ją z wartością podaną w wykazie. Oryginały plików pozostają zabezpieczone i mogą zostać udostępnione na każde żądanie organu.”

11. Najczęstsze błędy

Błąd	Skutek	Jak uniknąć
Zrzut tylko fragmentu ekranu bez URL	Brak dowodu, skąd pochodzi treść	Zawsze pełna strona + metryczka z URL
Domyślny szablon nagłówka FireShot (bez daty)	Brak daty i godziny na zrzucie	Stopka z %y-%m-%d %H:%M:%S (rozd. 4.2)
Poleganie na obiektach tekstowych z edytora	Edytowalne - łatwe do podważenia	Nagłówki/stopka nanoszone przy zapisie
Edycja oryginału (kadr, strzałki)	Hasz nieaktualny, zarzut manipulacji	Adnotacje tylko na kopiach roboczych
Hasz liczony po kilku dniach	Luka czasowa podważa integralność	Hasz natychmiast po zapisie
Brak kopii w Wayback	Tylko nasz materiał - słowo przeciw słowu	„Save Page Now” tego samego dnia
Zły zegar lub stara strefa w stopce	Rozbieżne godziny, podważenie wiarygodności	Synchronizacja czasu, zmiana CET/CEST

Wysyłka przez komunikator	Kompresja, utrata metadanych, nowy hasz	Przekazywanie oryginalnych plików
Jedna kopia na laptopie	Utrata dowodów przy awarii/kradzieży	Zasada 3-2-1
Tylko MD5/SHA-1	Algorytmy przestarzałe	SHA-256 jako standard
Selekcja plików przy zgrywaniu karty	Luki w numeracji, pytania „co usunięto?”	Kopiowanie całej karty

Załącznik A - Karta zabezpieczenia dowodu

Wypełnij jedną kartę dla każdego zabezpieczanego obiektu (strona www, sesja zdjęciowa, nagranie). Kartę można też prowadzić jako arkusz kalkulacyjny.

Nr dowodu (np. IEA-2026-015-W03)	
Sprawa / interwencja	
Rodzaj (strona www / zdjęcie / wideo / audio / pomiar / inne)	
Adres URL lub miejsce wykonania (adres, GPS)	
Data i godzina wykonania (ze strefą czasową)	
Narzędzie / urządzenie (np. FireShot Pro wersja ..., przeglądarka ...; aparat ..., nr seryjny)	
Osoba zabezpieczająca	
Świadek (imię, nazwisko, podpis)	
Nazwy plików oryginalnych	
SHA-256 plików oryginalnych	
Adres archiwalny Wayback Machine (i/lub archive.today)	
Godzina archiwizacji (UTC z adresu Wayback)	
Zakotwiczenie hasza w czasie (e-mail z dnia/godz., UPO, znacznik czasu)	
Miejsce przechowywania kopii 1 / 2 / 3	
Uwagi (np. zamknięto baner cookies, treść dynamiczna, logowanie)	
Przekazania (data - komu - forma - hasz przekazanego pliku)	

Podpis osoby zabezpieczającej	Podpis świadka

Załącznik B - Rejestr sum kontrolnych (manifest)

Lp.	Nr dowodu	Nazwa pliku	SHA-256	Data/god z. hasza	Wayback / uwagi
1	IEA-2026-015-W01	2026-09-28_073512_www.gmina.pl_Komunikat.pdf	3A7BD3E2...4F1B (pełne 64 znaki)	2026-09-28 07:37 CEST	web.archive.org/web/20260928053512/...
2	IEA-2026-015-W01	2026-09-28_073512_www.gmina.pl_Komunikat.png	...	...	jw.
3	IEA-2026-015-A01	ZOOM0042.WAV	...	...	pomiar nocny, ul. Leśna 5
4					
5					
6					

Wskazówka: w rejestrze zawsze wpisuj pełny 64-znakowy hasz. Skrócone formy (pierwsze i ostatnie 4 znaki) służą tylko do szybkiej orientacji. Wartości w przykładach są fikcyjne.

IEA poleca przygotowanie na bazie tej tabeli pliku Excel/Arkusza – wówczas długie ciągi znaków oraz wpisy rozkładają się bardziej czytelnie.

Załącznik C - Skrypty automatyzujące

C.1. Windows: manifest folderu

```
# Zapisz jako hasz.ps1; użycie: .\hasz.ps1 "C:\Dowody\Sprawa\01_ORYGINALY"
param([string]$Folder)
$out = Join-Path (Split-Path $Folder -Parent) "SHA256_manifest.csv"
Get-ChildItem $Folder -Recurse -File | ForEach-Object {
    [PSCustomObject]@{
        Plik    = $_.FullName
        Rozmiar = $_.Length
        SHA256  = (Get-FileHash $_.FullName -Algorithm SHA256).Hash
        Hasz_UTC = (Get-Date).ToUniversalTime().ToString("yyyy-MM-dd HH:mm:ss")
    }
} | Export-Csv $out -NoTypeInformation -Encoding UTF8 -Append
Get-FileHash $out -Algorithm SHA256
```

C.2. Windows: weryfikacja manifestu

```
Import-Csv "SHA256_manifest.csv" | ForEach-Object {
    $now = (Get-FileHash $_.Plik -Algorithm SHA256).Hash
    if ($now -eq $_.SHA256) { "OK    $_.Plik" } else { "ZMIANA! $_.Plik" }
}
```

C.3. Wayback Machine: zgłoszenie listy adresów

Najprościej: dla każdego adresu otworzyć w przeglądarce <https://web.archive.org/save/> + pełny URL. Dla zaawansowanych - API SPN2 (wymaga kluczy z konta archive.org) z parametrami `capture_screenshot=1` (zrzut), `capture_outlinks=1` (linki wychodzące) i `capture_all=1` (także strony z błędem 4xx/5xx).

```
# Linux/macOS - proste zgłoszenie listy adresów z pliku urls.txt
while read url; do
    curl -s -o /dev/null -w "%{http_code} $url\n" "https://web.archive.org/save/$url"
    sleep 20 # odstęp, aby nie przeciążyć archiwum
done < urls.txt
```

Po zgłoszeniu zawsze sprawdź ręcznie czy kopia jest poprawna, i zapisz adresy archiwalne.

Załącznik D - Szybka ściągą

Krok	Strona www	Własna dokumentacja (foto/wideo/audio)
0. Przygotowanie	Zegar zsynchronizowany; FireShot Pro: nagłówek „%t %u”, stopka „%y-%m-%d %H:%M:%S CEST osoba %p” (PDF i Images osobno); nazwa pliku „%y-%m-%d_%H%M%S_%e_%t”	Data/godzina/strefa w urządzeniach, GPS, puste karty, zdjęcie zegara referencyjnego
1. Utrwalenie	Pełna strona → PDF + PNG (bez edytora)	Slate na starcie, kontekst → szczegół, bez kasowania ujęć
2. Hasz	SHA-256 od razu po zapisie	Zgranie całej karty → manifest SHA-256
3. Niezależna kopia	web.archive.org/save → zapis adresu archiwalnego	E-mail z manifestem / UPO / znacznik czasu
4. Karta	Załącznik A + rejestr B	Załącznik A + rejestr B
5. Przechowywanie	01_ORYGINALY tylko do odczytu, 3-2-1	Jw. + metadane w 02_METADANE
6. Praca i przekazanie	Adnotacje na kopiach, pakiet z haszami	Montaż/anonimizacja na kopiach, hasz wersji finalnych

Kluczowe polecenia SHA-256:

Windows: certutil -hashfile plik SHA256 | Get-FileHash plik -Algorithm SHA256
 macOS: shasum -a 256 plik
 Linux: sha256sum plik | sha256sum -c SHA256SUMS.txt

„Dobre przygotowanie wiarygodnej dokumentacji dowodowej, to kluczowy element walki o swoje podstawowe prawa człowieka” - mecenas Magdalena Kozerska

Instytut Ekologii Akustycznej | instytut.ngo

Dokument udostępniony na licencji CC BY-SA 4.0 - dziel się nim ze swoją społecznością.



„Zabezpieczanie dowodów cyfrowych” - Klaudia Dąbrowska z Zespołem Obywatelskiej Akademii Ekologii Akustycznej, Instytut Ekologii Akustycznej, 2026 (instytut.ngo). Utwór udostępniony na licencji Creative Commons Uznanie autorstwa - Na tych samych warunkach 4.0 Międzynarodowe (CC BY-SA 4.0): <https://creativecommons.org/licenses/by-sa/4.0/deed.pl>

Możesz kopiować, rozpowszechniać, adaptować i wykorzystywać ten dokument, także w działaniach swojej społeczności - pod warunkiem podania autorstwa i źródła oraz udostępnienia wersji zmienionych na tej samej licencji. Postanowienie to ma pierwszeństwo przed domyślną licencją treści serwisu instytut.ngo.