BGService i ElView

Aktualizacja dokumentacji do wydania 3.1.94

Nowy serwis zgłoszeń EvidLock

Błędy modułów, funkcji i narzędzi, propozycje usprawnień oraz oceny można przekazywać przez bgservice.evidlock.pl. Serwis zastępuje opis wcześniejszej tablicy zgłoszeń w pomocy offline.

Bez logowania

Otwórz formularz zgłoszenia, wskaż moduł lub funkcję i opisz problem oraz kroki odtworzenia. **Wysłanie zgłoszenia nie wymaga konta ani logowania.**

Po zalogowaniu

Konto daje **własną tablicę zgłoszeń**, podgląd statusów oraz możliwość dopisywania notatek i uzupełnień. Logowanie odbywa się **bez hasła**: podajesz login i adres e-mail, a następnie kod jednorazowy otrzymany w wiadomości.

ElView: metadane zdjęcia

Opcja **Dane EXIF…** pokazuje pełne dane EXIF, GPS i IPTC/XMP bez uruchamiania pełnej analizy. Wynik można skopiować albo zapisać do TXT lub JSON. Poprawiono odczyt współrzędnych GPS, dat wykonania i danych aparatu; współrzędne można otworzyć na mapie OpenStreetMap.

ElView: wyszukiwanie obrazu w sieci

Opcja **Szukaj obrazu w sieci** obsługuje TinEye i PimEyes. Przekazanie obrazu wymaga potwierdzenia podstawy prawnej i zgody operatora; dla PimEyes wyświetlana jest dodatkowa informacja dotycząca danych biometrycznych.

Do wyszukiwania przygotowywana jest **przekodowana kopia bez EXIF**. Ma ona inną sumę SHA-256 niż oryginał, a dziennik zapisuje obie sumy. Dotyczy to wyszukiwania obrazu w ElView. Kopia wejściowa przekazana do ELSandbox powinna zachować sumę oryginału.

Funkcje ElView opisane powyżej pochodzą z wydania 3.1.91, a poprawki ELSandbox z 3.1.92 i 3.1.93. Wydanie 3.1.94 aktualizuje ich opis oraz historię online i offline.

ELSandbox
Instalacja i raport aktywnej sesji

Aktualizacja dokumentacji do wydania 3.1.94

WinError 32 podczas instalacji Visual C++ lub Npcap

Poprawiono przekazywanie polecenia instalacji w folderze współdzielonym. Program nie zmienia już nazwy pliku polecenia ani odpowiedzi w tym folderze. Skrypt gościa czeka na kompletny dokument, a panel ponawia odczyt chwilowo zablokowanego wyniku.

Po aktualizacji zamknij starą sesję i uruchom nową sesję ELSandbox. Najpierw zachowaj potrzebne wyniki. Już działająca piaskownica nadal ma poprzednie skrypty. Instalacja Visual C++ i Npcap odbywa się wyłącznie wewnątrz gościa.

Generuj raport HTML bez zamykania piaskownicy

Podczas aktywnej sesji kliknij **Generuj raport HTML** i wybierz miejsce zapisu. Raport zostanie oznaczony jako **częściowy - sesja w toku**. Pokazuje konfigurację, materiały przekazane jako kopie, dotychczasowy dziennik oraz bieżącą listę plików wynikowych. Piaskownica pozostaje uruchomiona.

Pliki wynikowe mogą być nadal zapisywane przez narzędzia w gościu. Raport częściowy pokazuje ich nazwy, rozmiary i daty modyfikacji bez obliczania SHA-256. **Po zakończeniu sesji wygeneruj nowy raport**, zawierający sumy plików wynikowych.

Jak porównywać sumy kontrolne

Sekcja **Materiały przekazane jako kopie** pokazuje SHA-256 materiału odczytanego podczas kopiowania. Tę wartość należy porównywać z sumą tego samego pliku na liście przekazywania do ELSandbox. Kopia wejściowa jest dodatkowo haszowana i weryfikowana.

Plik **raport.html.sha256** zawiera sumę samego raportu HTML. Sekcja **Trwałe wyniki** odnosi się do plików wynikowych z piaskownicy. Nie są to sumy oryginalnych materiałów wejściowych.

W razie rozbieżności zachowaj raport HTML oraz nazwę, pełną ścieżkę i obie porównywane sumy. Wydanie 3.1.94 nie zawiera deklarowanej naprawy nieodtworzonej rozbieżności sum materiałów wejściowych.

ELSandbox
Instalacja narzędzi i bibliotek

Uzupełnienie dokumentacji do wydania 3.1.94

Ten dodatek opisuje nowe funkcje ELSandbox. Za nim znajduje się dotychczasowa dokumentacja publiczna 3.1.72, zachowana bez zmian. Bieżąca historia wydań: evidlock.pl/changelog/.

Przygotowanie sesji

1. W sekcji **Trwałe wyniki** wybierz folder wyników przed uruchomieniem piaskownicy.
2. Wskaż Wireshark lub Procmon w sekcji **Narzędzia w piaskownicy**.
3. Uruchom nową sesję. Pobieranie instalatorów odbywa się na komputerze głównym, więc piaskownica może pozostać **offline**.

Błąd MSVCP140.dll: Visual C++

Kliknij **Zainstaluj Visual C++ w piaskownicy**. ELSandbox pobierze pakiet x64 Microsoft, sprawdzi podpis wydawcy i przekaże zweryfikowaną kopię do gościa. Instalacja odbywa się wyłącznie w piaskownicy. Poczekaj na wynik w panelu, a następnie ponownie uruchom Wireshark w gościu.

Przechwytywanie pakietów: Npcap

Kliknij **Zainstaluj Npcap w piaskownicy**. Program pobierze oficjalny instalator Npcap 1.89, sprawdzi podpis Nmap Software LLC i otworzy kreator wewnątrz piaskownicy. **W oknie gościa zaakceptuj licencję i wybierz opcje instalacji.** Po zakończeniu uruchom ponownie Wireshark i sprawdź listę interfejsów.

Npcap Free korzysta z interaktywnego kreatora; instalacja cicha jest funkcją OEM. Instalator jest pobierany bezpośrednio od producenta na żądanie i nie jest dołączany do wydania EvidLock.

„Nie można otworzyć tego linku https”

Taki komunikat po kliknięciu linku w Wiresharku oznacza brak aplikacji przypisanej do HTTPS w gościu. Użyj przycisku instalacji Npcap w panelu ELSandbox na komputerze głównym. Ten sposób **nie wymaga przeglądarki w piaskownicy**.

Wyniki i rozwiązywanie problemów

Co zostaje po instalacji

Wynik pojawia się w dzienniku panelu. W trwałym folderze wyników znajdują się **elsandbox_runtime_result.json** dla Visual C++ i **elsandbox_npcap_result.json** dla Npcap. Visual C++ zapisuje również **elsandbox_vcredist.log**. Są to dane diagnostyczne pochodzące z gościa.

Pobrane instalatory pozostają w pamięci podręcznej komputera głównego i przed ponownym użyciem są weryfikowane. Zamknięcie piaskownicy usuwa z niej zainstalowane składniki. **W każdej nowej sesji instalację trzeba powtórzyć.** Oba przyciski można uruchomić kolejno; każdy raz na sesję.

Znaczenie wybranych kodów

Składnik / kod	Znaczenie i dalsze działanie
Visual C++ / 0	Instalacja zakończona. Uruchom ponownie Wireshark.
Visual C++ / 1638	Instalator zgłasza inną, już zainstalowaną wersję.
Npcap / 1	Użytkownik anulował kreator instalacji.
Npcap / 350	Instalacja wymaga restartu i ponowienia.
Oba / 3010	Instalacja zakończona, wymagany restart. Npcap może nie być jeszcze gotowy do przechwytywania.

Nie zamykaj piaskownicy w celu „zachowania” instalacji: nowa sesja zacznie od czystego systemu. Brak wyniku po 10 minutach nie oznacza przerwania instalatora; sprawdź jego okno w gościu.

Oficjalne źródła pobierania

Microsoft Visual C++ x64

Wireshark

Npcap

Process Monitor (Procmon)

Npcap: instrukcja i kody wyniku

Przyciski „pobierz” w ELSandbox otwierają przeglądarkę komputera głównego. Samo mapowanie folderu Wiresharka nie przenosi bibliotek i sterowników hosta. Bez Npcap można analizować zapisane pliki PCAP/PCAPNG.



EvidLockV2

Dokumentacja techniczna i eksploatacyjna

Wersja 3.1.72 · wydanie publiczne

AUTOR

CybF1sh

EvidSec · evidsec.pl

www.evidlock.pl

2026

EvidLockV2 3.1.72

Dokumentacja techniczna i eksploatacyjna

Wydanie dokumentu: 11 września 2026 r. Dokument opracowany od nowa na podstawie aktualnego repozytorium, konfiguracji wydawania, testów oraz rzeczywistych okien programu. „EvidLockV2" jest nazwą produktu; numer przygotowywanego wydania to **3.1.72**. SUITE i PRO oznaczają uprawnienia licencyjne, a Install i Portable - sposób dystrybucji. Wyniki wcześniejszych prób są oznaczone numerem rzeczywiście badanego pliku.

Dokument opisuje zachowanie aplikacji i sposób jej utrzymania. Bieżący stan gotowych paczek oraz publikacji jest zapisany oddzielnie w `STATUS_WYDANIA.md`. Sama obecność numeru w repozytorium nie potwierdza wersji wszystkich plików EXE.

Nowe ilustracje wykonano bezpośrednio w skompilowanym **EvidLock Install 3.1.72**, uruchomionym z `dist/installer/universal/EvidLockV2/EvidLockV2.exe`. Widoki ElCommander, ElNotes, ElVoice i ElPlayer przedstawiają moduły tego instalacyjnego wydania. Nie są makietami ani zrzutami starych instalatorów modułów. Dane przykładowe są syntetyczne; pliki znajdują się w katalogu `examples` obok dokumentu.

Wydanie publiczne. Pominięto w nim informacje przeznaczone wyłącznie dla wydawcy: obsługę panelu licencji i generatora kluczy oraz procedurę budowania i publikacji wydań. Pozostała treść odpowiada pełnej dokumentacji wydania 3.1.72.

Zmiany po wydaniu 3.1.72. Dokument opisuje wersję 3.1.72; zrzuty i wyniki testów pochodzą z tej wersji. Kolejne wydania wprowadziły poprawki, które zmieniają część opisanych zachowań:

- **3.1.73** - tryb wysokiego kontrastu znów buduje pełny dashboard. Portable ONEDIR i SFX przy pierwszym uruchomieniu po aktualizacji przywracają z kopii poprzedniej wersji klucz ELP1, licznik uruchomień i dziennik błędów przechowywane w `_runtime`; istniejące pliki nie są nadpisywane. Gotowe EXE korzystają z historii zmian wbudowanej w kompilację.
- **3.1.74** - aktualizacja wersji instalowanej kończy się instalacją i pokazuje każdy etap: postęp pobierania, okno instalatora, a po ponownym uruchomieniu wynik aktualizacji albo przyczynę niepowodzenia ze ścieżką dziennika instalacji. Błędy aktualizacji trafiają do dziennika błędów aplikacji. W Portable wymiana czeka na zamknięcie programu bez limitu czasu, a wymiana katalogu ONEDIR kończy się w całości albo przywraca poprzednią wersję.

Pełna lista zmian: www.evidlock.pl/changelog/.

Spis treści

1. Produkty, licencje i składniki 4

2. Uruchomienie i główne okno 5

3. Architektura i odpowiedzialność kodu 6

4. Dane, sprawy i kontrola integralności 7

5. Cztery moduły dystrybuowane samodzielnie 8

6. Pozostałe moduły głównego programu 14

7. Klucze produktu i aktywacja 16

8. TeamServer PRO 17

9. Aktualizacje online i offline 20

10. Diagnostyka 21

11. Walidacja i granice potwierdzenia 21

12. Źródła i materiały kontrolne 22

1. Produkty, licencje i składniki

EvidLock służy do organizacji spraw, zabezpieczania plików, kontroli integralności, analizy materiałów cyfrowych oraz przygotowywania wyników i raportów. Główny program i samodzielne moduły korzystają z tego samego drzewa kodu `evidence_locker`.

1.1. SUITE i PRO

Możliwość	SUITE	PRO
Główny EvidLockV2	Tak	Tak
ElCommander, ElNotes, ElVoice, ElPlayer	Tak	Tak
Praca lokalna i lokalne dane spraw	Tak	Tak
Współpraca przez TeamServer	Nie	Tak
Automatyczne doinstalowanie funkcji pominiętych w Portable	Nie	Nie
Dostarczony i skonfigurowany hosting TeamServera	Nie wynika z klucza	Nie wynika z klucza

PRO obejmuje SUITE i dodaje TeamServer. Historyczny identyfikator `all` w podpisie klucza i bazie oznacza obecnie SUITE. Nie nadaje uprawnień do TeamServera. Interfejs generatora oferuje nazwy SUITE oraz PRO; alias techniczny nie jest trzecią ofertą.

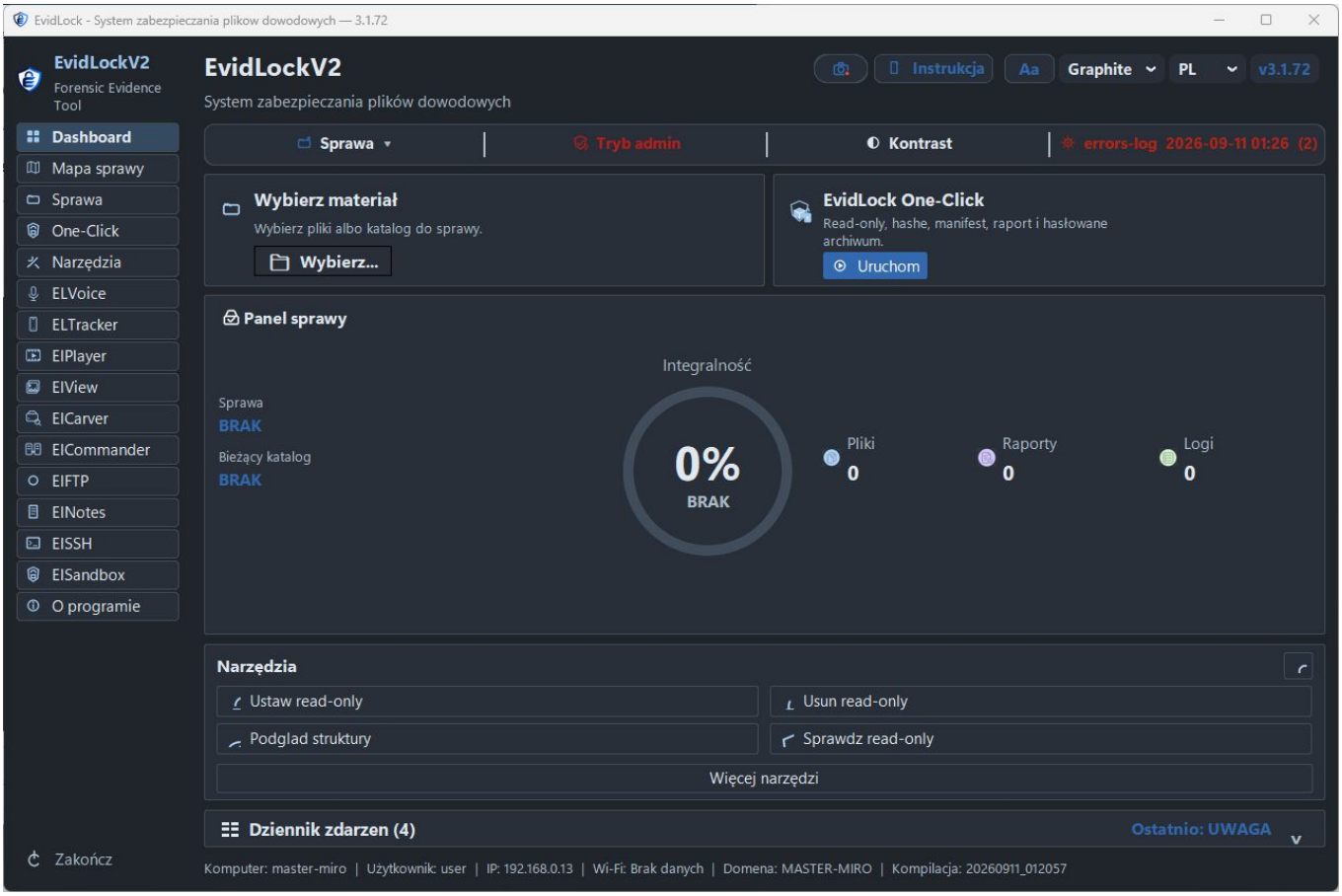
1.2. Formaty dystrybucji

Wariant	Zawartość i sposób uruchomienia
Install Universal	Pełny instalator z wyborem składników; może zawierać wszystkie moduły, w tym ElVoice i ElPlayer. Faktyczny wybór opisuje `components.ini`.
Portable Light ONEDIR	Katalog z launcherem `EvidLock.exe` i obowiązkowym `_runtime`. Trzeba przenosić cały katalog.
Portable Light ONEFILE	Jeden plik dystrybucyjny, rozpakowujący runtime do pamięci podręcznej przy uruchomieniu.
Portable Light SFX	Samorozpakowujące opakowanie ONEDIR. Po rozpakowaniu obowiązują zasady ONEDIR.
Cztery instalatory modułów	Osobne produkty ElCommander, ElNotes, ElVoice i ElPlayer. Każdy wymaga klucza SUITE albo PRO.

Portable Light jest okrojony. Profil wyklucza interfejsy ElVoice, ElPlayer, ElSSH i moduł OCR oraz ciężkie zależności, m.in. Torch, SciPy i Whisper. Nie jest zamiennikiem pełnego Install. ElNotes może korzystać z lokalnie dostępnego Tesseract; obecność przycisku OCR nie dowodzi obecności silnika. Paramiko i zależności SFTP pozostają w profilu Portable. Programy TeamServera i zależności PostgreSQL nie są częścią tego profilu.

Samodzielny ElCommander obejmuje także integracje ElFTP i ElNotes oraz narzędzia 7-Zip/FFmpeg. ElNotes ma własny instalator; ElFTP i ElSSH nie mają odrębnych pozycji w katalogu produkcyjnych instalatorów. Generator kluczy jest prywatnym narzędziem wydawcy.

2. Uruchomienie i główne okno



Nowy zrzut: Dashboard, bez otwartej sprawy. Numer wydania jest widoczny w prawym górnym rogu.

Lewy panel przełącza Dashboard, mapę sprawy, sprawę, One-Click, narzędzia i dostępne moduły. Panel środkowy pokazuje aktywną sprawę, bieżący katalog, stan integralności i liczniki. Brak sprawy i zerowe liczniki oznaczają pusty kontekst, nie pomyślną weryfikację dowodów. Dolny dziennik przedstawia zdarzenia aplikacji.

W 3.1.72 wskaźnik został powiększony do pola 176 px. Tytuł znajduje się nad pierścieniem, a większy procent i status w środku. Cieńsza obwódka korzysta z palety wybranego motywu.

Procent jest **ważonym stanem kompletności czynności w sprawie**, a nie odsetkiem poprawnie zahashowanych plików. Wagi wynoszą: sygnatura 15, nośnik 10, materiał 25, manifest 10, zabezpieczenie materiału 25, dokumentacja 5 i weryfikacja integralności 10. Status OK daje pełną wagę, UWAGA jej 45%, INFO 20% (części są zaokrąglane w dół do punktów). Kolor zielony zaczyna się od 95%, pomarańczowy od 50%, niższy wynik jest czerwony; brak danych ma kolor neutralny. Ocena nie zastępuje odczytu raportu weryfikacji.

Podstawowy przebieg pracy:

1. Zweryfikować wersję, licencję oraz wymagane składniki. Uruchomić właściwy wariant programu.
2. Utworzyć lub otworzyć sprawę i wybrać katalog wynikowy. Wyniki powinny znajdować się poza źródłem.
3. Wybrać pliki lub katalog źródłowy, zanotować ich pochodzenie i parametry pozyskania.
4. Wykonać kontrolę integralności lub odpowiednią operację modułu. Sprawdzić log, pominięte elementy i błędy odczytu.
5. Otworzyć wynik, porównać oczekiwane dane i zachować raport wraz z parametrami oraz sumami.

Tryb administratora jest potrzebny dla niektórych czynności systemowych, np. dostępu do urządzeń czy usług. Podniesienie uprawnień UAC nie izoluje programu od systemu. Programowe RO i ochrona operacji w interfejsie nie zastępują sprzętowego blokera zapisu.

3. Architektura i odpowiedzialność kodu

Start prowadzi przez `evidlockv2.py`, `evidence_locker/startup_loader.py` i `evidence_locker/app.py`. Aplikacja zestawia funkcje zależnie od profilu, licencji, składników i trybu uruchomienia. Samodzielny moduł korzysta ze wspólnego hosta GUI, uruchamiając wybrane narzędzie.

Warstwa lub plik	Odpowiedzialność
`app.py`, `startup_loader.py`, `runtime.py`	Start, kontekst aplikacji, inicjalizacja i zgodność starszych interfejsów
`features/`, `views/`, `controllers/`	Widoki, polecenia i koordynacja działań użytkownika
`services/`	Parsowanie, hashowanie, formaty, analiza, eksporty, procesy zewnętrzne
`models/`, `repositories/`	Struktury danych i zapis
`platform/`, `security/`	Integracja systemowa, ścieżki, uprawnienia i procesy
`module_registry.py`	Rejestr modułów, akcji i zależności narzędziowych
`runtime.py`, `features/lifecycle.py`, `app.py`	Wybór i uruchomienie produktów modułowych oraz ich procesów
`product_license.py`, `portable_license.py`	Weryfikacja podpisanych kluczy i stan aktywacji
`update_integration.py`, `evidlock_updater.py`	Integracja aktualizacji, pobranie i instalacja
`technical_docs.py`	Wbudowana pomoc offline, odrębna od tego dokumentu zewnętrznego

Jest to architektura modułowa z warstwą zgodności i mixinami. Nazwy katalogów nie oznaczają ścisłego MVC. Dłuższe operacje są wykonywane w zadaniach i procesach, a GUI odbiera wynik; czas reakcji na anulowanie zależy od konkretnej operacji i narzędzia zewnętrznego.

Zmian nie wykonuje się w wygenerowanym `moduels_install/_engine`. Źródłem modułów jest repozytorium. `engine_source.json` oraz podpisane inwentarze kompilacji wiążą gotowe pliki z odciskiem źródeł.

4. Dane, sprawy i kontrola integralności

Sprawa wiąże materiał, metadane, notatki, zdarzenia, wyniki i raporty. Źródło, kopia robocza i eksport są różnymi artefaktami. Dokumentowanie operacji powinno obejmować ścieżkę źródła, moment odczytu, narzędzie i jego wersję, parametry, wynik oraz błędy.

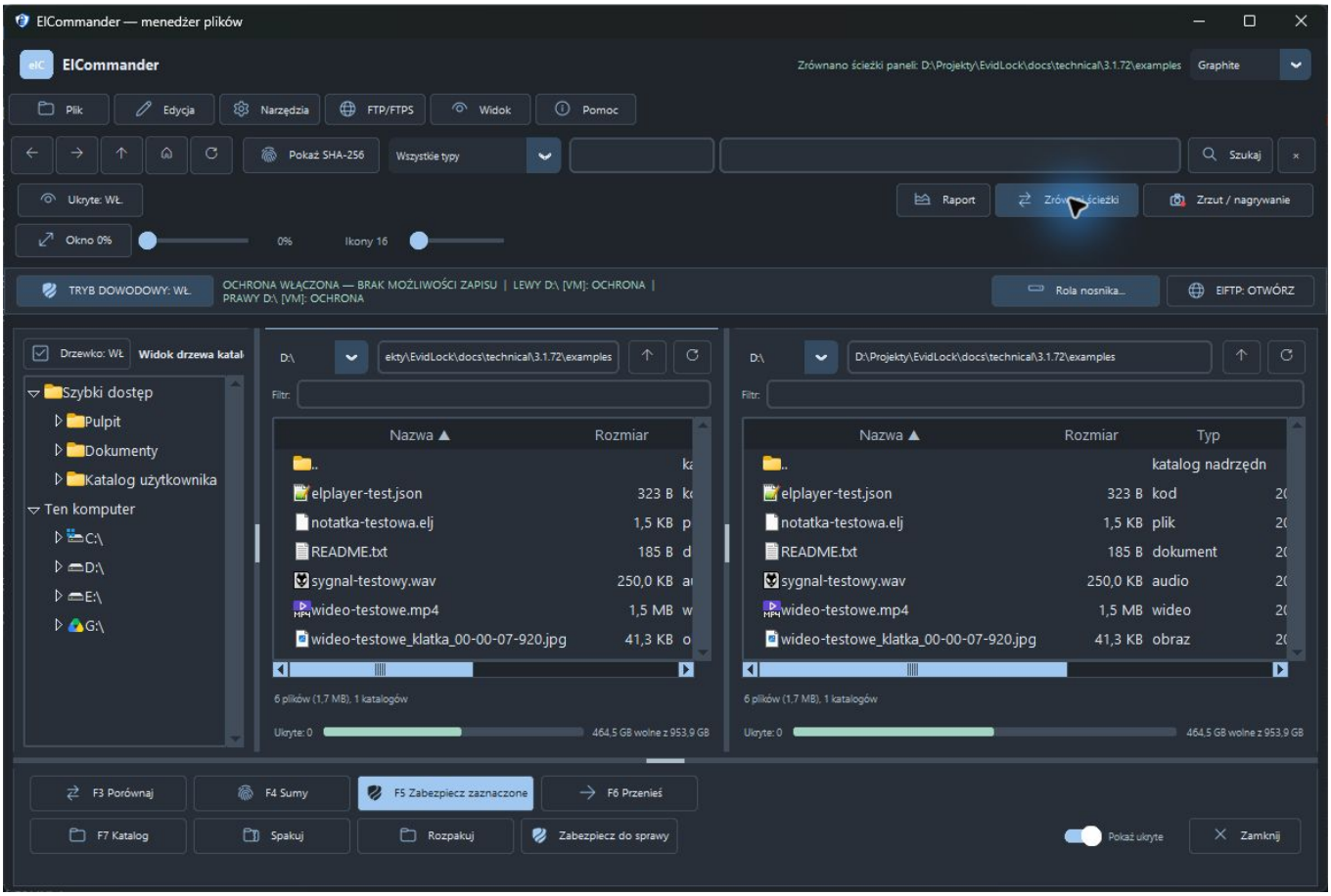
SHA-256 identyfikuje zawartość pliku. BLAKE3 jest opcją szybkiej inwentaryzacji, a MD5 służy zgodności z innymi narzędziami. Zgodna suma nie potwierdza autorstwa ani prawdziwości opisu materiału. Manifest porządkuje rekordy zbioru; wynik trzeba odczytywać łącznie z informacją o plikach niedostępnych i pominiętych.

Lokalna tablica ustaleń korzysta z SQLite/WAL i schematu 3. Stany obejmują `draft`, `pending_review`, `verified`, `approved`; lokalne role to `admin`, `analyst`, `reviewer`, `reader`. Autor nie powinien sam weryfikować i zatwierdzać własnego ustalenia. Łańcuch hashy umożliwia sprawdzenie spójności zdarzeń, ale nie jest niezależnym znacznikiem czasu.

Praca lokalna i TeamServer są odrębnymi trybami. Utworzenie SQLite nie konfiguruje serwera PostgreSQL. Poświadczenia serwera, hasło konta zespołu, hasło notatki ELJ i klucz produktu są odrębnymi sekretami o różnych zastosowaniach.

5. Cztery moduły dystrybuowane samodzielnie

5.1. ElCommander - pliki i transfery



Oba panele wskazują katalog syntetycznych przykładów. Tryb dowodowy jest włączony. Na zrzucie potwierdzono nawigację i zrównanie ścieżek.

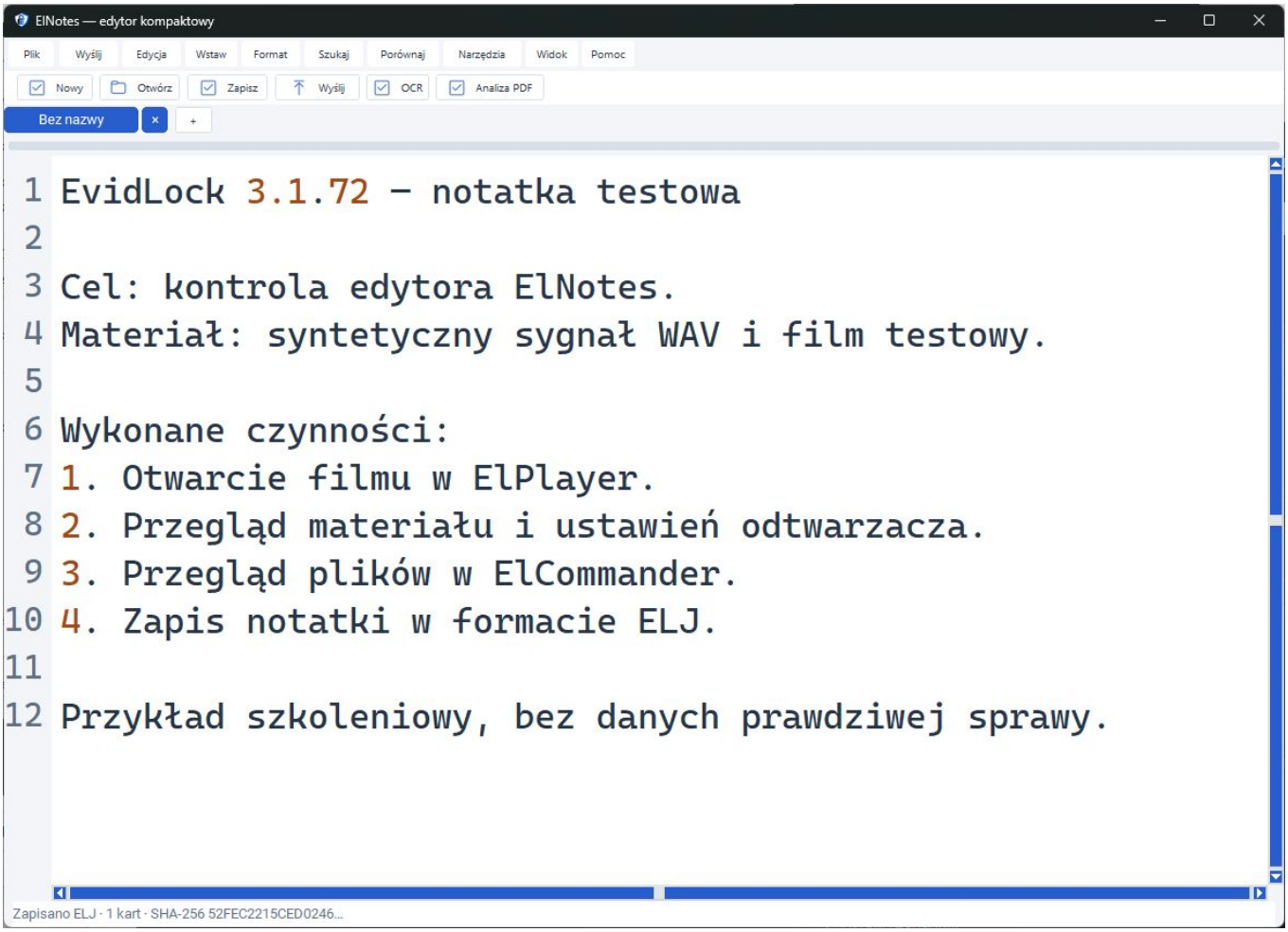
Dwupanelowy menedżer udostępnia przegląd katalogów, filtrowanie, porównania, sumy kontrolne, kopiowanie, przenoszenie, archiwa, podglądy i zabezpieczanie materiału do sprawy. Akcje zapisu mogą zmieniać pliki - należy odczytywać status ochrony i rolę nośnika przed ich uruchomieniem.

Przykład kontroli pliku: przejść do katalogu, zaznaczyć plik, wybrać „F4 Sumy" albo „Pokaż SHA-256", a wynik porównać z niezależnym zapisem. „Zrównaj ścieżki" zmienia katalog panelu, nie synchronizuje zawartości dysków. Przy kopiowaniu do sprawy należy sprawdzić zarówno rezultat, jak i log operacji.

ElFTP otwiera klienta transferów. FTP/FTPS i SFTP są różnymi protokołami; SFTP korzysta z Paramiko. Rodzaj połączenia i sposób weryfikacji serwera wynikają z profilu. Udany start okna nie jest testem połączenia z dowolnym serwerem. Dołączane narzędzia obejmują 7-Zip i FFmpeg.

Inspekcja linków PDF jest statyczna: nie uruchamia JavaScript, nie otwiera połączeń sieciowych i nie wykonuje OCR. Limity tej operacji to 64 MiB pliku, 2000 stron, 30000 obiektów, 5000 wyników, głębokość 40 i budżet 30 s. Budżet jest kooperacyjny, a nie izolacją parsera w oddzielnym procesie.

5.2. ElNotes - notatki, kod i ELJ



Nowy zrzut po zapisie notatki do `examples/notatka-testowa.elj`. *Wygląd odzwierciedla ustawienia lokalnego edytora: jasny motyw i powiększony tekst.*

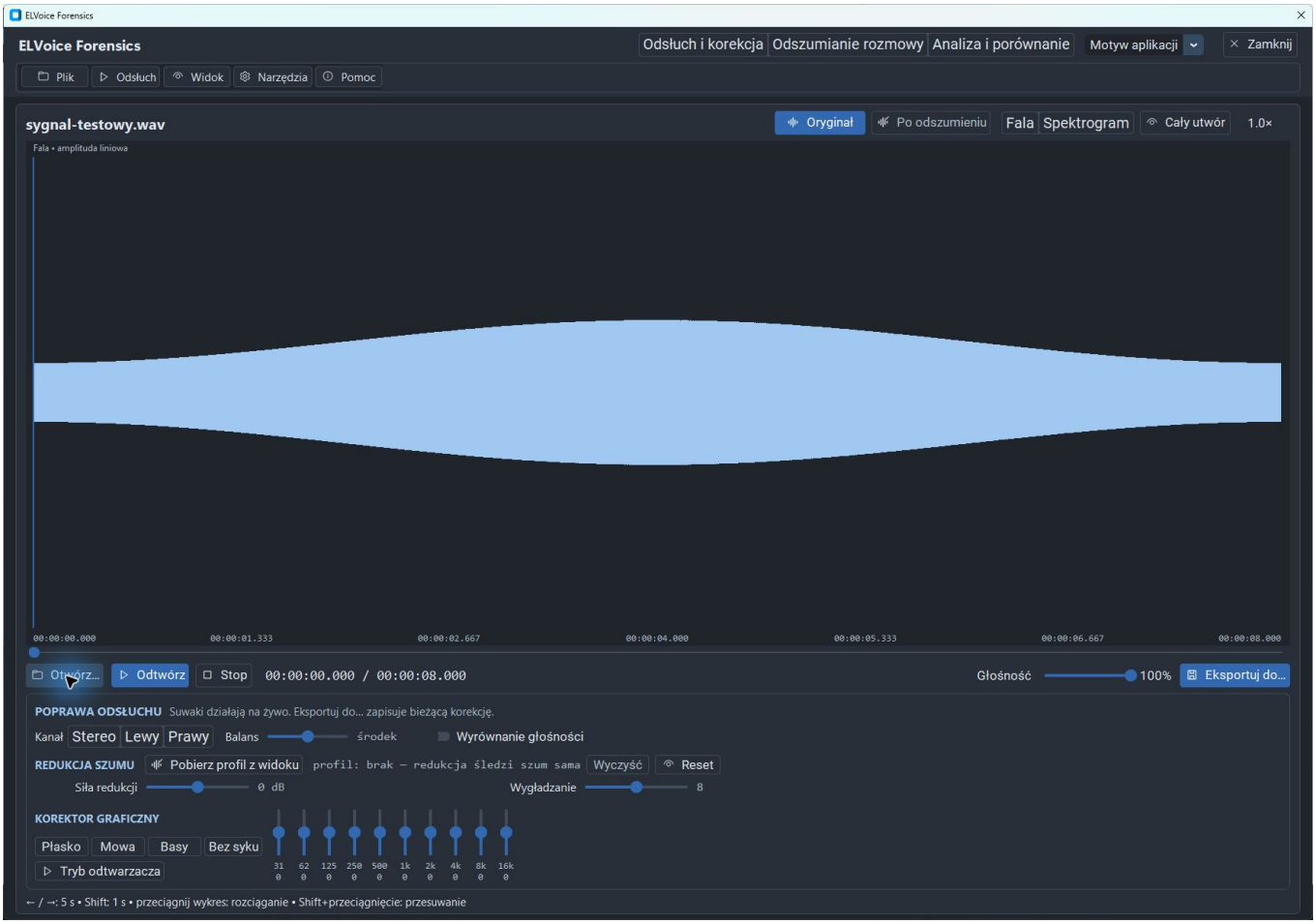
ElNotes oferuje karty, edycję tekstu i kodu, wyszukiwanie, porównanie, podgląd Markdown, funkcje PDF oraz OCR zależny od silnika. Menu i dodatkowe paski udostępniają format zapisu, kodowanie, końce wierszy i narzędzia. Zwykły plik tekstowy i pełna przestrzeń ELJ mają różną zawartość.

Przestrzeń `.elj` przechowuje karty, wygląd, metadane i załączniki. Sygnatura to `EVIDELJ\x1a`, wersja formatu 1.0. Kontener sprawdza strukturę, indeks i sumy. Opcjonalne zabezpieczenie hasłem używa AES-256-GCM oraz PBKDF2-HMAC z 600000 iteracji. Klucz SUITE/PRO nie odszyfrowuje notatki i nie zastępuje jej hasła.

Limity odczytu ELJ: 4096 elementów, 256000000 bajtów pojedynczego elementu, 768000000 bajtów łącznie po rozwinięciu i współczynnik kompresji 500. Import zwykłego tekstu ma osobny limit 32 MiB. Limit nie oznacza gwarantowanej płynności pracy dla największego dokumentu.

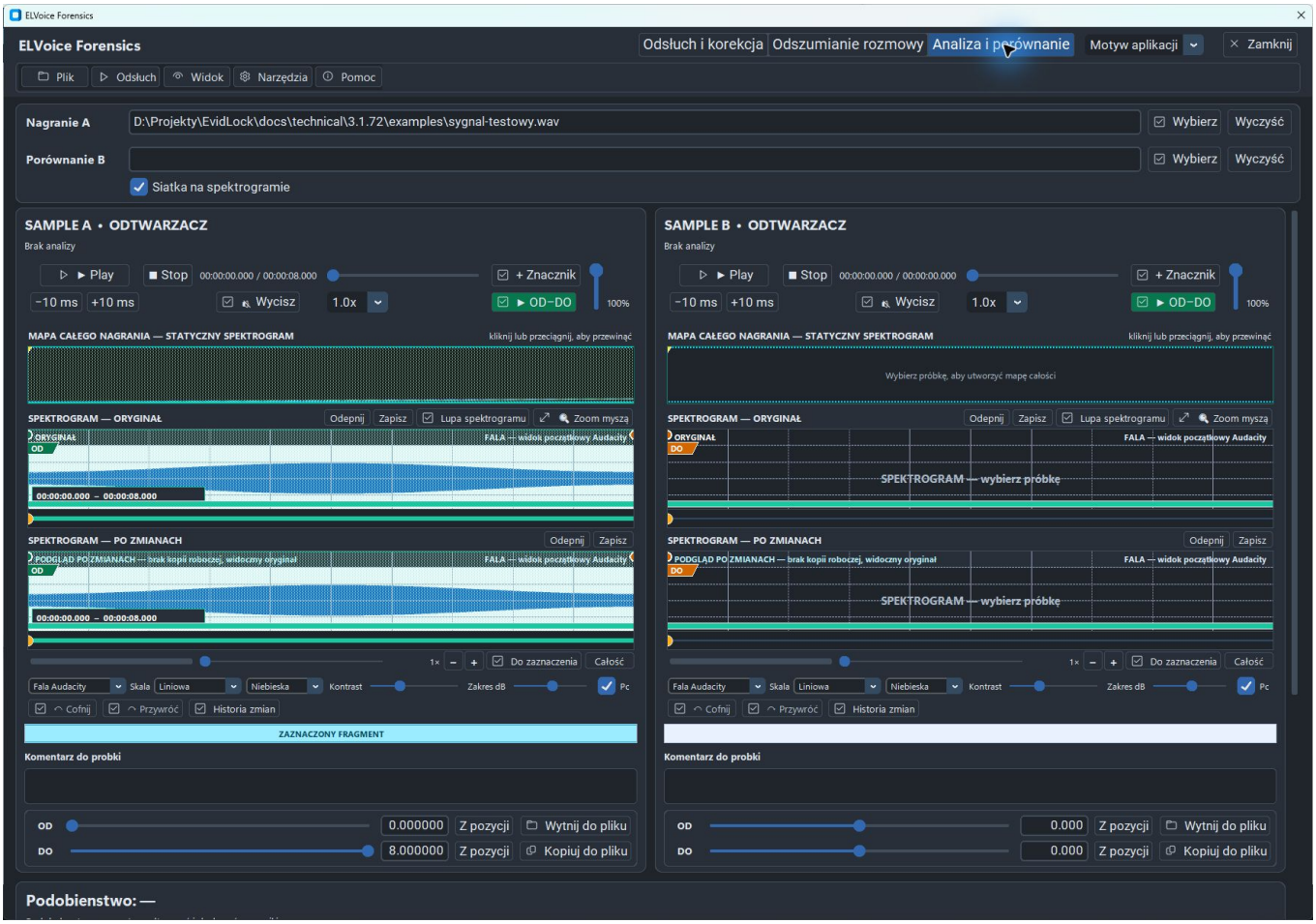
Przykład zapisu: utworzyć kartę, wprowadzić tekst, wybrać „Zapisz”, wskazać `.elj` i zdecydować o ochronie hasłem. Przykład dokumentacyjny zapisano bez hasła, ponieważ nie zawiera danych sprawy. Odczyt przez parser potwierdził jedną kartę, wersję źródłową 3.1.72 i zachowanie polskich znaków. Eksport PDF wymaga osobnej kontroli układu i kompletności.

5.3. ElVoice - odsłuch i analiza audio



Wczytany syntetyczny sygnał WAV. Przycisk „Reset" znajduje się przy „Wyczyść", w obszarze opcji odsłuchu.

ElVoice pokazuje przebieg sygnału, umożliwia odsłuch, analizę i porównanie próbek oraz korekcję dźwięku. Obszar poprawy odsłuchu obejmuje kanały, balans, wyrównanie głośności, redukcję szumu i korektor. „Wyczyść" dotyczy profilu szumu; „Reset" służy przywróceniu ustawień korekcji. Eksport zapisuje przetworzony wynik jako oddzielny materiał.

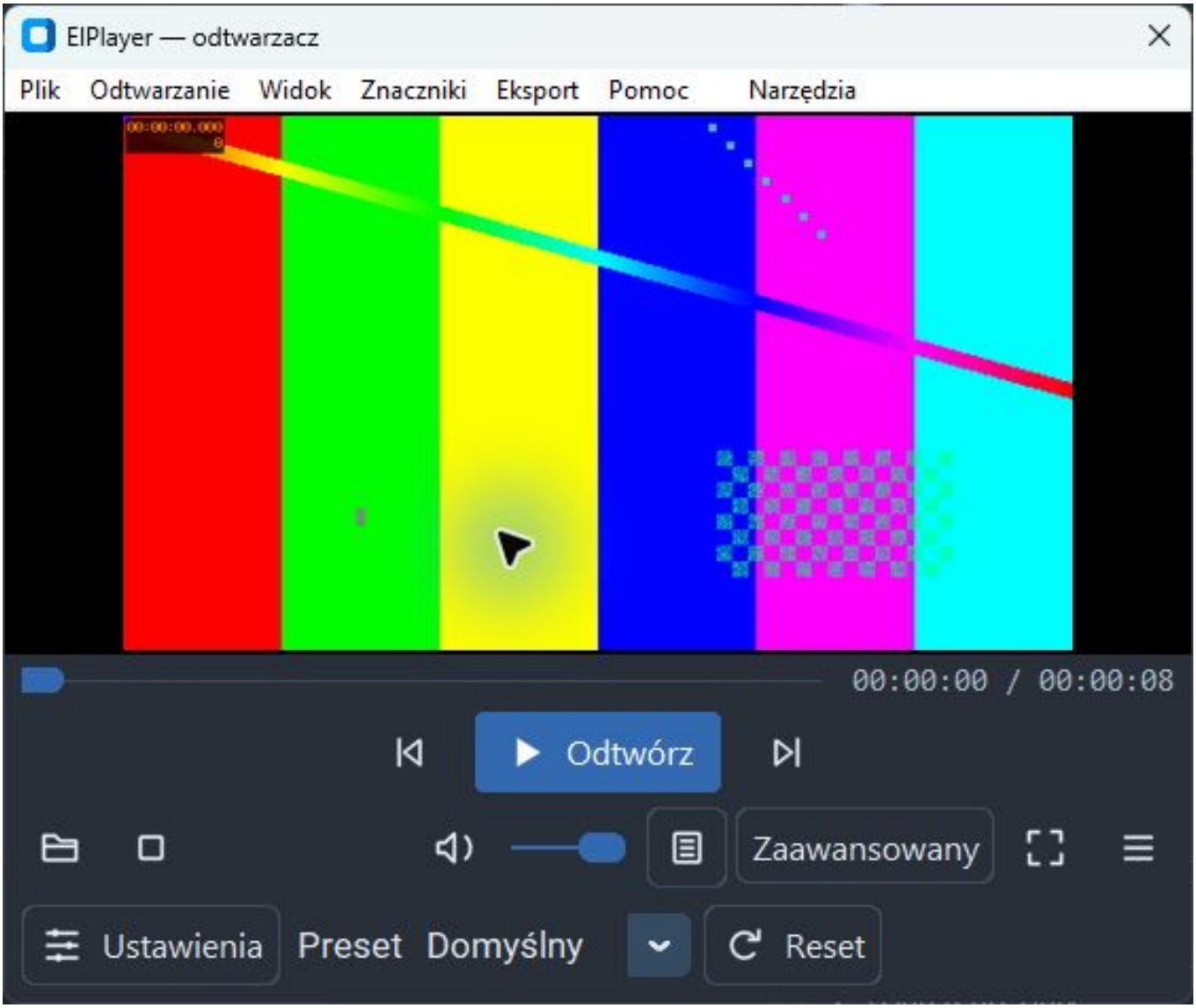


Widok porównania z materiałem A. Puste pole B i komunikat o braku analizy nie przedstawiają wyniku porównania.

Przebieg pracy: otworzyć audio, sprawdzić długość i przebieg, odsłuchać, dobrać ustawienia, a następnie wyeksportować wynik do nowego pliku. Dla porównania trzeba wczytać oba materiały i uruchomić analizę. Podobieństwo cech sygnału nie jest identyfikacją biometryczną mówcy.

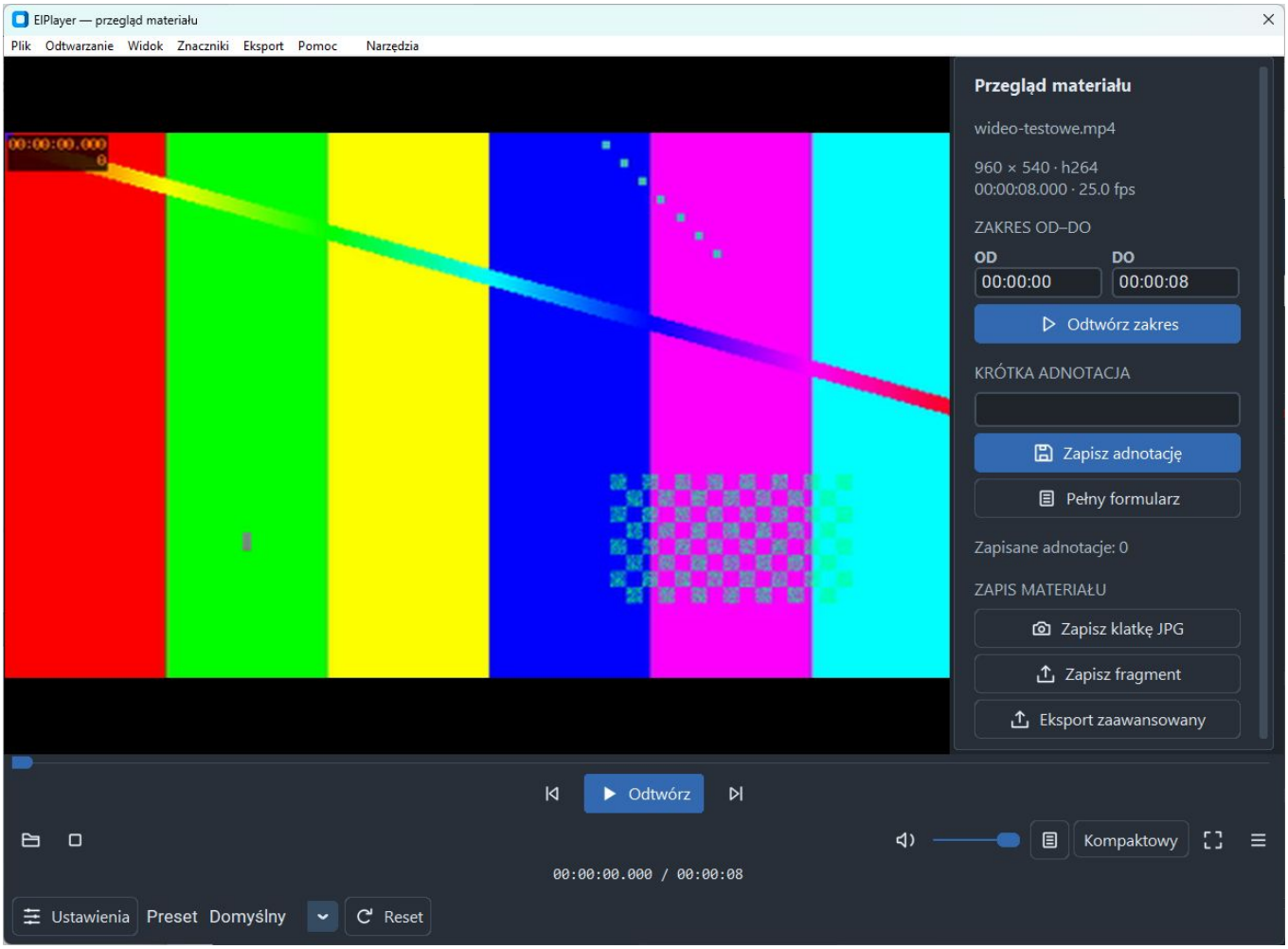
Dekodowanie korzysta z FFmpeg. Lokalna transkrypcja korzysta z whisper.cpp i odpowiedniego modelu; jest to inny komponent niż biblioteka Python Whisper. Brak modelu lub runtime uniemożliwia tę funkcję. Transkrypcję należy sprawdzić z nagraniem. Syntetyczny sygnał użyty w dokumentacji nie zawiera mowy i nie służy do oceny jej rozpoznawania.

5.4. ElPlayer - odtwarzanie i eksport



Przycisk odtwarzania ma niebieski kolor zgodny z kontrolkami ElVoice; poprzedni zielony przycisk zastąpiono.

ElPlayer odtwarza audio i wideo, udostępnia sterowanie klatkami, zakres OD-DO, zrzuty, eksport fragmentów, metadane i adnotacje. Widok przeglądu pokazuje więcej narzędzi niż odtwarzacz kompaktowy.



Testowy film: 960 × 540, 25 klatek/s, 8 s. Plansza i dźwięk powstały syntetycznie.

Przykład: otworzyć film, wybrać „Odtwórz”, zatrzymać w wybranym miejscu i wyeksportować klatkę JPG. W tej sesji sprawdzono rzeczywiste odtwarzanie, zmianę przycisku na pauzę oraz eksport klatki przy pozycji 7,92 s. Zapisany JPG ma rozmiar 960 × 540. Plik i metadane kontroli znajdują się w `examples`.

Czas materiału zależy od znaczników czasu strumienia. Dla wideo ze zmiennym klatkażem nie wolno bez sprawdzenia zastępować go ilorazem numeru klatki i nominalnego FPS. FFmpeg/ffprobe oraz dekodery określają obsługę formatów. Eksport tworzy oddzielny artefakt; należy zapisać jego parametry i sumę.

6. Pozostałe moduły głównego programu

Rejestr obejmuje 26 identyfikatorów modułów. Tabela opisuje zakres kodu; dostępność na stanowisku zależy od Install/Portable, zaznaczonych składników i narzędzi. Nie wszystkie pozycje są osobnymi aplikacjami do pobrania.

Identyfikator	Zadanie	Główna zależność lub ograniczenie
`storage_info`	Informacje o dyskach i woluminach	Uprawnienia systemowe i dostęp do urządzenia
`windows_logs`	Odczyt zdarzeń Windows	Dostępność i poprawność źródła EVTX
`disk_imaging`	Obrazy nośników i montowanie	ImDisk, uprawnienia, właściwy tryb RO/RW
`system_audit`	Audyt informacji systemowych	Zakres uprawnień i dostępnych artefaktów
`profiling`	Profilowanie i korelacja zdarzeń	Poprawność danych i stref czasowych
`evidence_graph`	Graf relacji materiału	Relacja nie jest automatycznym dowodem przyczynowym
`case_analysis`	Analiza danych sprawy	Kontekst i kompletność zebranych informacji
`plaso`	Zadania osi czasu Plaso	Oddzielny runtime lub kontener narzędzia
`browser_forensics`	Artefakty przeglądarek	Kopie profili, dostęp do baz i parsery
`image_forensics`	Analiza obrazów	Formaty i dekodery
`memory_forensics`	Pozyskanie i analiza RAM	WinPmem/Volatility, administrator i zgodność obrazu
`registry`	Analiza rejestru Windows	Dostęp do właściwych plików i kluczy
`case_backup`	Kopie danych sprawy	Osobne miejsce zapisu i sprawdzenie odtworzenia
`pdf_tools`	Operacje na PDF	Format dokumentu, limity parsera
`ocr`	Rozpoznawanie tekstu	Tesseract; moduł wykluczony z Portable Light
`elnetwork`	Analiza materiału sieciowego	Narzędzia Wireshark; brak automatycznego odszyfrowania TLS
`elvoice`	Analiza audio	FFmpeg i narzędzia/model transkrypcji; brak w Portable Light
`eltracker`	Artefakty urządzeń i kopii mobilnych	Obsługiwany format kopii i parser
`elplayer`	Odtwarzanie i analiza audio/wideo	FFmpeg; brak w Portable Light
`elview`	Podgląd obrazów i metadanych	Pillow/HEIF i dostępne dekodery
`elcarver`	Wyszukiwanie i odzyskiwanie plików	Odzysk może być fragmentaryczny

Identyfikator	Zadanie	Główna zależność lub ograniczenie
`elcommander`	Menedżer plików	7-Zip, FFmpeg i zależności transferów
`elssh`	Sesje SSH	Integracja z ElCommander; brak w Portable Light
`elnotes`	Tekst, kod, PDF, ELJ	Dodatkowe silniki dla wybranych funkcji
`elsandbox`	Sesja Windows Sandbox dla kopii pliku	Funkcja Windows, wirtualizacja i konfiguracja mapowań
`archive_tools`	Archiwa	7-Zip; RAR wymaga odpowiedniego dekodera

Plaso wymaga sprawdzenia runtime, wersji obrazu, mapowań źródła i katalogu wynikowego. Konfiguracja źródła powinna zachowywać `source_read_only: true`. Samo wygenerowanie konfiguracji nie jest testem działania parserów. Docker Desktop na badanym stanowisku zgłaszał błąd inicjalizacji `dockerInference`; nie wykonywano resetu fabrycznego. TeamServer został przetestowany bez Dockera. Nie potwierdzono tym samym gotowości Plaso w Dockerze.

7. Klucze produktu i aktywacja

7.1. Format i zaufanie

Klucz ma postać `ELP1.<payload-base64url>.<signature-base64url>`. Podpis Ed25519 jest sprawdzany publicznym kluczem osadzonym w kliencie. Payload opisuje schemat, identyfikator, klienta, edycję, liczbę stanowisk, datę wystawienia i opcjonalną datę ważności. Dla Portable może zawierać kod urządzenia `ELUSB1…` lub dopuszczony wariant `ANY`.

Weryfikator sprawdza strukturę, podpis, typy pól, edycję, termin ważności oraz związanie z urządzeniem, gdy ma zastosowanie. Wartość `seats` opisuje limit licencji, lecz klient offline nie prowadzi centralnego licznika uruchomionych stanowisk. Nie należy utożsamiać pola w kluczu z egzekwowaniem jednoczesnych sesji przez serwer.

Odcisk istniejącego wydawcy produktów: `ELPK1-2406-9BB0-3F6A-7D24-5668-0B27-5572-8CB3`. Zmiana nazwy ALL na SUITE nie wymagała wymiany klucza kryptograficznego. Prywatny klucz wydawcy nie może znaleźć się w instalatorze klienta, katalogu publicznym WWW ani dokumentacji.

7.2. Aktywacja w aplikacji

Program określa produkt i dystrybucję, odczytuje zapisany klucz, weryfikuje go, a następnie ustala uprawnienia. Gdy wymaga wprowadzenia klucza, użytkownik wkleja pełny klucz SUITE lub PRO i zatwierdza zapis. Aplikacja odczytuje zapisany stan ponownie; sam pomyślny wynik parsowania nie zastępuje udanego zapisu.

Install preferuje aktywację użytkownika w `%LOCALAPPDATA%\EvidLock\license` przed współdzieloną lokalizacją ProgramData. Portable stosuje lokalizację powiązaną z nośnikiem i katalog `EvidLockData\license`; szczegóły zależą od uruchomienia z nośnika wymiennego lub dysku lokalnego. Przenoszenie licencji związanej z urządzeniem na inny nośnik wymaga zgodnego klucza.

Przy starcie usuwana jest odziedziczona zmienna `EVIDLOCK_LICENSE_EDITION`, aby stan innego procesu nie przenosił uprawnień PRO. Lokalny stan próbny, tam gdzie udostępnia go dany profil, jest mechanizmem niezależnym od klucza produktu.

8. TeamServer PRO

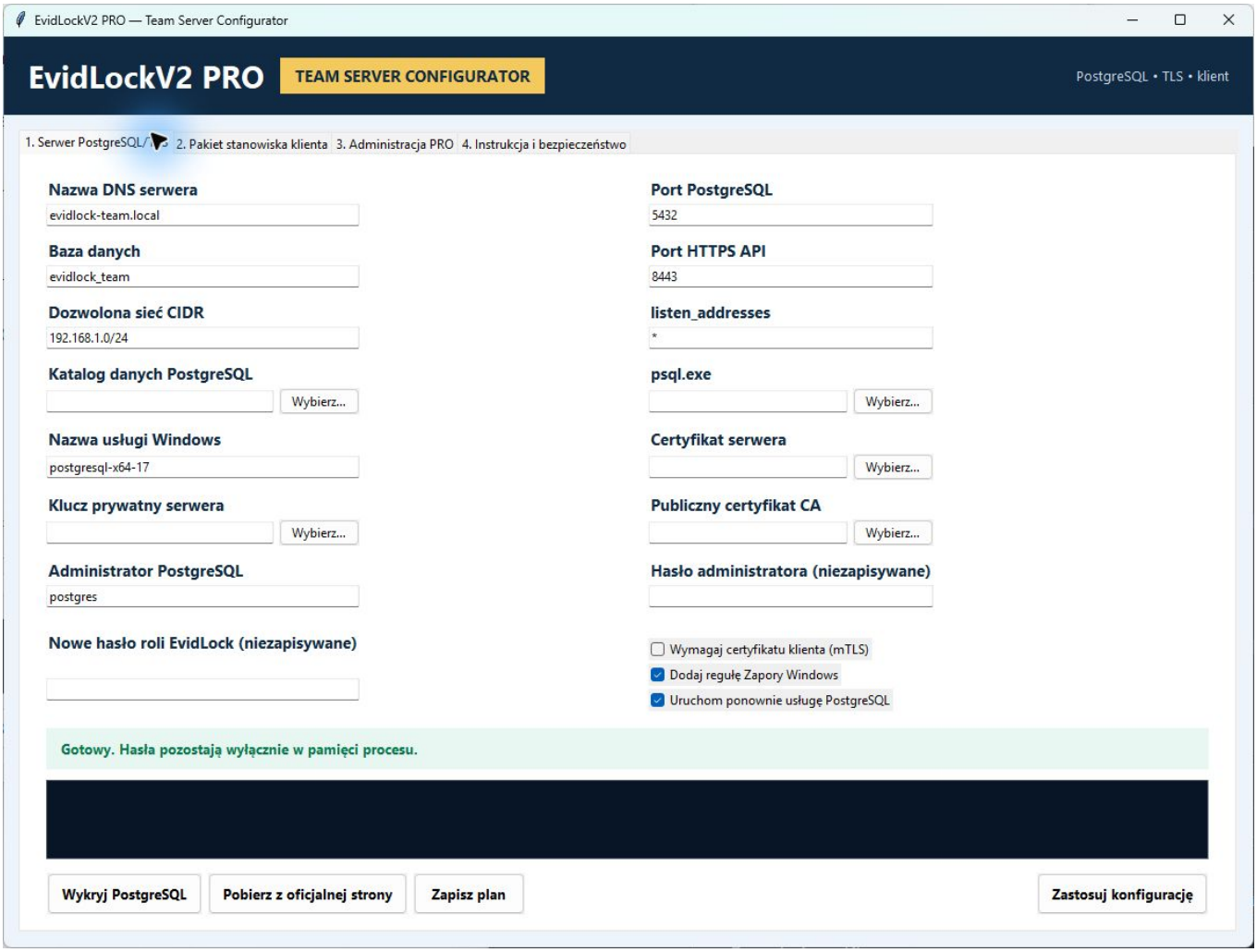
8.1. Składniki i połączenia

TeamServer zapewnia współpracę przez HTTPS i PostgreSQL. Klient wymaga PRO; SUITE nie odblokowuje połączenia zespołowego. Konfigurator, konsola i usługa to osobne pliki w pełnym wydaniu Install:

- `EvidLockTeamServerConfigurator.exe` - konfiguracja graficzna;
- `EvidLockTeamServerConsole.exe` - polecenia administracyjne i diagnostyka;
- `EvidLockTeamServerService.exe` - host Windows Service Control Manager.

Domyślne wartości konfiguratora to port PostgreSQL **5432**, port HTTPS API **8443**, baza `evidlock_team` i rola aplikacyjna `evidlock`. To wartości początkowe, a nie wykryta konfiguracja konkretnej sieci. Usługa API nasłuchuje na `0.0.0.0`; dostęp trzeba ograniczyć właściwą zaporą. Połączenie z PostgreSQL używa `sslmode=verify-full` i wskazanego CA.

8.2. Przygotowanie serwera



1. Przygotować serwer Windows, PostgreSQL, katalog danych i kopii oraz konto administracyjne do instalacji. Dobrać nazwę DNS, porty i dozwoloną sieć.
2. Dostarczyć certyfikat serwera, odpowiadający mu klucz prywatny i certyfikat CA. Nazwa używana przez klienta musi odpowiadać certyfikatowi. Certyfikat localhost użyty w testach nie jest certyfikatem produkcyjnym.

3. W konfiguratorze wykryć instalację PostgreSQL, wskazać narzędzia i katalog danych, przygotować oraz przejrzeć plan. Zweryfikować ograniczenia sieci i ustawienia TLS przed zastosowaniem.
4. Zastosować plan, zainicjalizować bazę i schemat Enterprise, utworzyć konto administratora i skonfigurować MFA tam, gdzie wymagane.
5. Przygotować konfigurację API i zarejestrować usługę z odpowiednimi uprawnieniami. Sprawdzić start i stan usługi.
6. Przygotować profil klienta z adresem HTTPS i CA, połączyć dwa konta PRO i sprawdzić zapis, odczyt oraz odmowę zapisu dla konta tylko do odczytu.
7. Wykonać i odtworzyć zaszyfrowaną kopię do oddzielnej bazy testowej. Dopiero po kontroli danych odebrać wdrożenie.

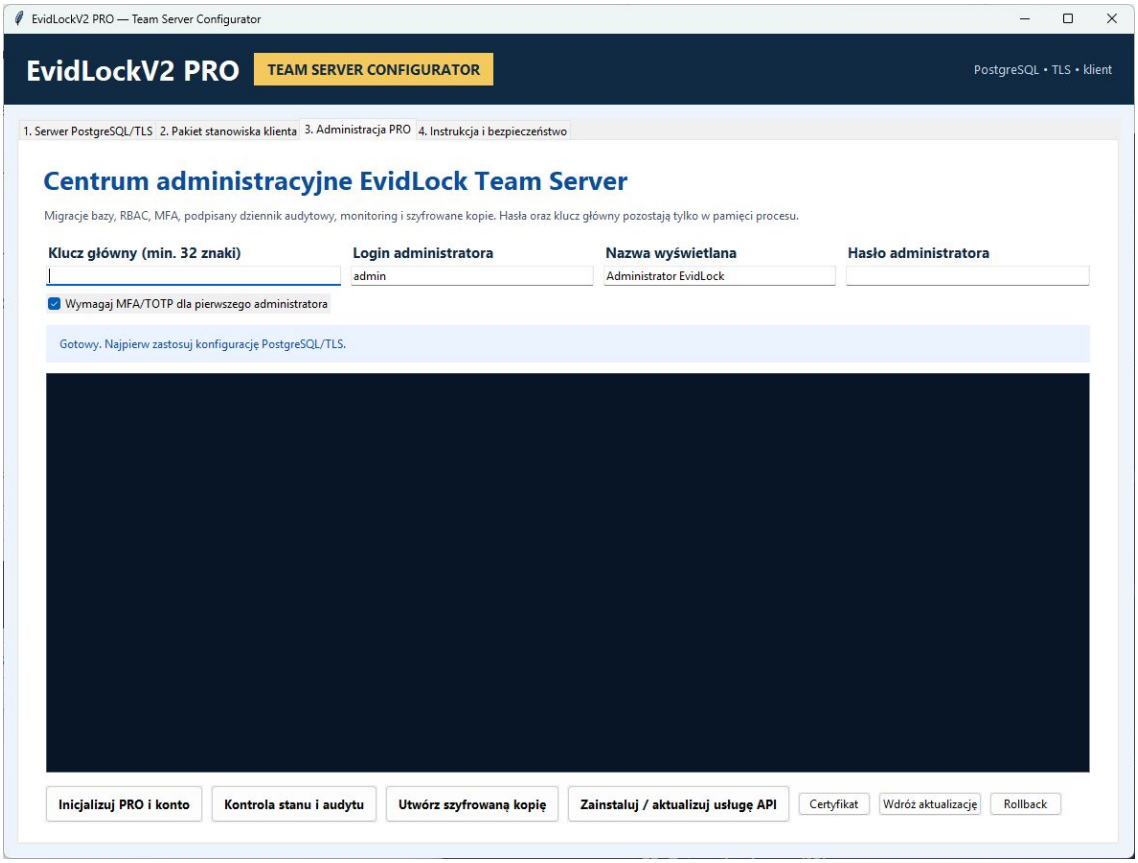
Konsola udostępnia m.in. `detect`, `plan`, `apply`, `client-bundle`, `enterprise-init`, `create-admin`, `health`, `backup`, `restore`, `serve-api`, `install-api-service`, `remove-api-service` i `self-test`. Pełny zestaw argumentów należy odczytać przez `--help`. Dla haseł preferować odczyt interaktywny; argumenty polecenia mogą być widoczne w historii i liście procesów.

8.3. Konfiguracja usługi i sekrety

Domyślny katalog to `%PROGRAMDATA%\EvidLock\TeamServer`. Plik `server.json` zawiera konfigurację połączeń i ścieżek, a `server.secrets.dpapi` - hasło bazy i klucz główny chronione Windows DPAPI w zakresie komputera. Kod próbuje nadać katalogowi ACL dla SYSTEM i administratorów. Wynik ACL trzeba sprawdzić przy odbiorze, ponieważ wywołanie `icacls` nie wymusza przerwania przy błędzie.

DPAPI w zakresie komputera wymaga ochrony dostępu do pliku; nie zastępuje ACL. Skopiowanie zaszyfrowanego pliku na inny komputer nie jest kompletną procedurą odtworzenia. Klucz główny i poświadczenia muszą mieć sprawdzony, niezależny plan odzyskiwania.

8.4. Role, konflikty i audyt



Role Enterprise obejmują `server_admin`, `case_admin`, `analyst`, `reviewer`, `read_only` i `auditor`. Dostęp do widoku administracyjnego nie daje automatycznie prawa do jego zmiany. Zmiana kanałów aktualizacji wymaga administratora serwera. Rozwiązanie konfliktu jest kontrolowane po stronie API i wymaga uprawnionej roli; konta tylko do odczytu nie mogą wykonać tej operacji.

Współbieżne zapisy mogą utworzyć konflikt wersji. Serwer zachowuje dane i wymaga rozstrzygnięcia przez uprawnionego użytkownika. Audyt normalizuje daty do UTC; dopisywanie do łańcucha jest szeregowane blokadą transakcyjną PostgreSQL, aby dwa zapisy nie wykorzystały tego samego poprzedniego hasha.

Kopia wykorzystuje `pg_dump`, szyfrowanie i odtworzenie przez `pg_restore`. Poprawny wynik zapisu kopii nie wystarcza: trzeba sprawdzić odszyfrowanie, odtworzenie notatek i spójność audytu. Kopii bazy nie należy utożsamiać z pełną kopią systemu, certyfikatów i konfiguracji usługi.

8.5. Co potwierdzono testem

Rzeczywisty test uruchomił odizolowany PostgreSQL 17.11 oraz serwer HTTPS i dwa klienty. Potwierdził TLS, migracje, logowanie, odmowę błędnego hasła i MFA, poprawne TOTP, synchronizację notatek, sygnatury z polskimi znakami, powiadomienia, kontrolę ról, konflikt i rozwiązanie, osiem równoczesnych dopisań audytu oraz zaszyfrowaną kopię i odtworzenie do drugiej bazy. Błędny klucz kopii został odrzucony.

Oddzielny test prawdziwej usługi Windows obejmuje rejestrację w SCM, start, uwierzytelniony odczyt HTTPS, stop, ponowny start i kolejny odczyt. Na końcu usuwa wyłącznie własną usługę i konfigurację testową. Wersję badanego pliku i wynik powtórzenia dla bieżącej paczki podaje `STATUS_WYDANIA.md`.

To test kompletnej lokalnej ścieżki działania, nie odbiór sieci klienta, Active Directory, firmowego CA, kont domenowych ani zachowania podczas awarii całego hosta. Tych scenariuszy nie przedstawiamy jako sprawdzonych.

9. Aktualizacje online i offline

9.1. Model zaufania

Pierwsze wydanie jest dystrybuowane bez Authenticode zgodnie z decyzją właściciela. Windows może pokazać nieznanego wydawcę. Aktualizacje mają niezależny podpis **Ed25519 manifestu**, a pliki są sprawdzane po rozmiarze i SHA-256. Podpis manifestu nie zastępuje podpisu Windows ani reputacji SmartScreen.

Publiczny klucz aktualizacji jest osadzony w `update_trust.py`. Podpis obejmuje kanoniczny JSON bez pola `signature`: uporządkowane klucze, ASCII escapes, separatory przecinek/dwukropek, bez NaN. Podpis ma algorytm Ed25519 i wartość Base64. Klucz dostarczony razem z pobranym manifestem nie może zastąpić klucza zaufanego klienta.

Odcisk SHA-256 publicznego klucza aktualizacji: `ca6d2fe02c12f351dae4b1cfd5a8b7c1009d80773688431e05e2d9c8e65d15fb`. Prywatny klucz podpisujący aktualizacje nie jest publikowany. To osobna tożsamość niż klucz produktów.

9.2. Online

Klient przekazuje rzeczywistą wersję, produkt, dystrybucję i PID. Pobiera manifest HTTPS z dozwolonego hosta, weryfikuje podpis, tożsamość produktu i nowszą wersję. Dobiera właściwy format, pobiera plik i sprawdza rozmiar oraz sumę. Następnie uruchamia instalator lub przygotowuje wymianę Portable po zamknięciu aplikacji.

Produkt	Kanał
Install Universal	`https://updates.evidlock.pl/stable/universal/latest.json`
Portable Light	`https://updates.evidlock.pl/stable/universal/portable.json`
ElCommander	`https://updates.evidlock.pl/stable/elcommander/latest.json`
ElNotes	`https://updates.evidlock.pl/stable/elnotes/latest.json`
ElVoice	`https://updates.evidlock.pl/stable/elvoice/latest.json`
ElPlayer	`https://updates.evidlock.pl/stable/elplayer/latest.json`

Limit manifestu to 1 MiB, a pliku pobieranego 3 GiB. Lista dozwolonych hostów obejmuje także końcowy adres pobrania. Wersja równa lub starsza nie jest proponowana. Dostępność strony głównej HTTP 200 nie potwierdza działania kanału ani pobrania instalatora.

9.3. Portable i wycofanie nieudanej wymiany

ONEFILE wymienia pojedynczy EXE i zachowuje `.previous`. ONEDIR przyjmuje ZIP z `EvidLock.exe` i `_runtime/`. Odrzuca wyjście poza katalog, alternatywne strumienie NTFS, zastrzeżone nazwy i duplikaty. Maksimum to 30000 elementów i 12 GiB po rozwinięciu. Staging `.evidlock-update-*` powstaje na tym samym woluminie.

Po zamknięciu procesu poprzednie pliki trafiają do `.evidlock-previous-*`, nowe są wstawiane i uruchamiany jest launcher. Przy błędzie przenoszenia pomocnik podejmuje próbę przywrócenia poprzednich plików. Dane i licencja poza runtime nie podlegają wymianie. Nie jest to gwarancja atomowości przy dowolnej awarii zasilania. Poprzednią kopię należy zachować do odbioru nowej wersji.

SFX nie aktualizuje się jako archiwum leżące na dysku; aktualizacji podlega jego rozpakowany ONEDIR. Przeniesienie samego launchera ONEDIR lub zastąpienie runtime pojedynczym EXE nie jest obsługiwanym sposobem aktualizacji.

9.4. Offline

`.elupdate` to ZIP z podpisanym `update-package.json` i wskazanym artefaktem. Weryfikacja obejmuje podpis, produkt, wersję, rozmiar i SHA-256, tak jak online. Paczkę należy dostarczyć w całości i uruchomić przez funkcję aktualizacji offline. Uszkodzenie podpisu albo próba użycia paczki innego produktu ma zakończyć się odmową.

Stary klient wymagający Authenticode może potrzebować ręcznej migracji przez nowy, zweryfikowany instalator. Nie należy zakładać, że każdy dawny aktualizator zaakceptuje nowy protokół wyłącznie po zmianie pliku na serwerze.

10. Diagnostyka

Objaw	Sprawdzenie i działanie
SUITE nie łączy z TeamServerem	Wymagany PRO. SUITE obejmuje pracę lokalną i moduły.
PRO, lecz brak ElVoice/ElPlayer	Sprawdzić Portable Light oraz wybrane składniki Install. Klucz nie dostarcza bibliotek.
Portable ONEDIR nie startuje po skopiowaniu EXE	Przywrócić cały katalog `_runtime` z tego samego wydania.
Transkrypcja niedostępna	Sprawdzić whisper.cpp, model, ścieżki i log. Odsłuch nie potwierdza gotowości transkrypcji.
OCR niedostępny	Sprawdzić profil i silnik Tesseract; obecność GUI nie potwierdza instalacji zależności.
Aktualizacja HTTP 503	Sprawdzić tryb konserwacji i komplet publikacji. Nie usuwać markera przed przygotowaniem paczek.
Błąd podpisu lub sumy aktualizacji	Nie instalować pliku; sprawdzić wersję manifestu, zaufany klucz i komplet transferu.
TeamServer: błąd TLS	Sprawdzić DNS, ważność i nazwy certyfikatu, CA, zegar, porty i zaporę.
Usługa startuje i kończy działanie	Sprawdzić runtime DPAPI/ACL, ścieżki certyfikatów, bazę i diagnostykę SCM.
Błąd odczytu zaszyfrowanego ELJ	Sprawdzić właściwe hasło i integralność. Klucz produktu nie odzyskuje hasła.
Konflikt współpracy	Zachować wersje, sprawdzić uprawnienia i rozstrzygnąć przez właściwą rolę.
Docker `dockerInference`	Jest to błąd środowiska Docker; lokalne testy TeamServera nie wymagają jego resetowania.

11. Walidacja i granice potwierdzenia

Wyniki należy rozdzielać według poziomu: test źródeł, test skompilowanego programu, ręczna kontrola interfejsu, instalacja i publikacja. Przejście jednego poziomu nie dowodzi pozostałych.

W tej pracy przeszły zestawy testów licencji i generatora, kontrola panelu PHP i CSRF, integracja PostgreSQL/HTTPS, test usługi Windows oraz testy aktualizatora i wymiany ONEDIR na kontrolowanych artefaktach. Testy CLI prywatnego generatora potwierdziły wystawianie kluczy SUITE i PRO. Zestaw Portable zawierał 212 testów zakończonych pomyślnie.

Ręczne kontrole 3.1.72 obejmują uruchomienie Dashboardu i czterech modułów, większy wskaźnik integralności, wczytanie audio i filmu, położenie Reset, kolor Play, nawigację ElCommander oraz zapis/odczyt ELJ z polskimi znakami. Odtwarzanie filmu i eksport JPG 960×540 sprawdzono wcześniej w kompilacji 3.1.70; ten osobny wynik zachowuje rzeczywisty numer badanego programu. Skompilowany walidator 3.1.72 przeszedł 48 prób licencji, a usługa TeamServer 3.1.72 przeszła start, odczyt HTTPS, stop i restart z kolejnym odczytem. Oryginalne zrzuty są w `screenshots`, a dane

kontrolne w `examples`.

Wybrane zestawy nie są pełnym wynikiem całego CI. Wcześniejszy audyt architektury wskazał trzy niezgodności starych założeń testów: punkt wejścia, import Tk w pomocniku testowym i sposób zapisu wersji. Dokument nie przedstawia ich jako naprawionych. Nie wykonano walidacji wszystkich parserów na pełnym katalogu formatów ani odbioru infrastruktury konkretnego klienta.

Ostateczne wyniki kompilacji, instalatorów, podpisanych kanałów i pobrań HTTPS są zebrane w `STATUS_WYDANIA.md`. Należy używać ich łącznie z tą dokumentacją, zamiast wnioskować o zakończeniu publikacji ze zrzutu działającego programu.

12. Źródła i materiały kontrolne

Główne kontrakty w repozytorium: `supported_releases.json`, `moduels_install/modules.json`, `module_registry.py`, `portable_light_profile.py`, `product_license.py`, `portable_license.py`, `update_integration.py`, `update_trust.py`, `evidlock_updater.py`, `services/portable_update_package.py`, `services/team_server_runtime_config.py`, `services/team_server_enterprise_service.py`, `services/team_server_api_client.py` i `services/elnotes_service.py`.

Zrzuty bieżącego dokumentu i przykłady są niezależnym, jawnym materiałem dokumentacyjnym. Żaden plik dokumentacji nie zawiera klucza prywatnego wydawcy, hasła bazy ani kopii dziennika licencji.