23 Deszyfrowanie danych, plików, dysków

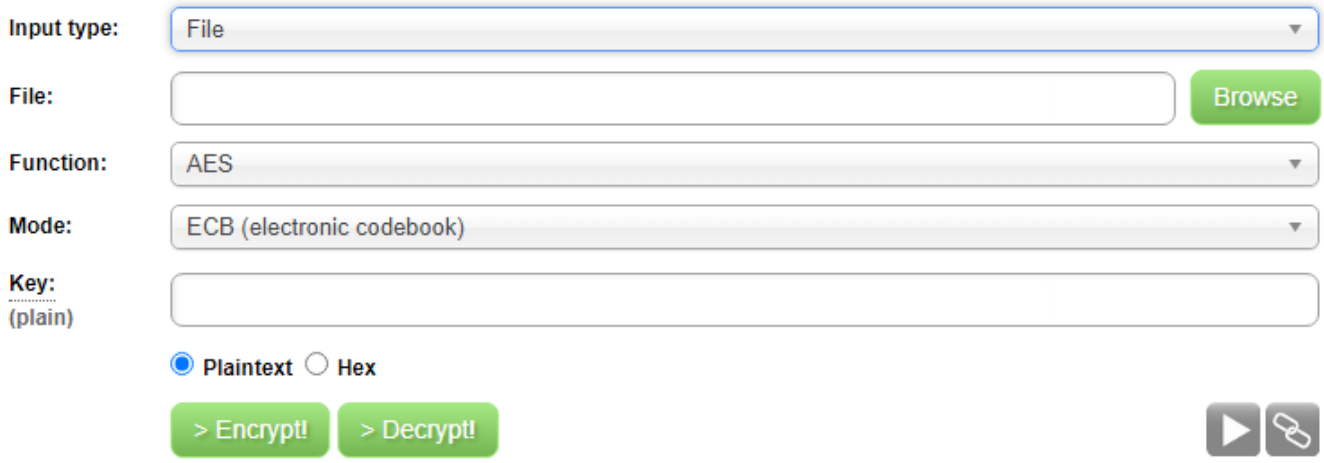
Część 1. Jak odszyfrować plik online bez klucza/certyfikatu/hasła

Możesz odszyfrować plik online bez klucza, jeśli masz odpowiednie narzędzie. Advanced Encryption Standard (AES) to algorytm szyfrowania symetrycznego. Poniżej znajduje się przykład generowania hasła zaszyfrowanego AES i odszyfrowania hasła zaszyfrowanego AES.

Advanced Encryption Standard (AES) to algorytm szyfrowania symetrycznego. AES jest obecnie standardem branżowym, ponieważ umożliwia szyfrowanie 128-bitowe, 192-bitowe i 256-bitowe. Szyfrowanie symetryczne jest bardzo szybkie w porównaniu z szyfrowaniem asymetrycznym i jest stosowane w systemach takich jak system baz danych. Poniżej znajduje się narzędzie online do generowania zaszyfrowanego hasła AES i odszyfrowywania zaszyfrowanego hasła AES. Zapewnia dwa tryby szyfrowania i deszyfrowania w trybie EBC i CBC.

Za pomocą narzędzie online do szyfrowania i deszyfrowania AES (kalkulator) dostępnego poniżej wykonaj:

a) szyfrowanie krótkiego tekstu i przykładowego pliku, który znajduje się w folderze.
b) deszyfrowanie szyfrowanie krótkiego tekstu i przykładowego pliku, który znajduje się w folderze.



Wykonaj powyższe czynności korzystając z jednej z stron

http://aes.online-domain-tools.com/

https://www.devglan.com/online-tools/aes-encryption-decryption

https://www.javainuse.com/aesgenerator

https://aesencryptiondecryption.tool-kit.dev/

http://ieasynote.com/tools/aes

gdyby wszystkie nie działały to wpisz w przeglądarkę online-tools aes-encryption-decryption

Jeśli potrzebujesz odszyfrować pliki, wiele przewodników doradzi Ci wypróbowanie narzędzi do odszyfrowywania online. Musisz jednak mieć świadomość, że te narzędzia nie są w 100% bezpieczne. Możesz być narażony na kradzież danych lub uszkodzenie danych źródłowych.

Instrukcja użytkowania strony poniżej

Wszelkie dane wejściowe lub wyjściowe w postaci zwykłego tekstu, które wprowadzasz lub generujemy, nie są przechowywane w tej witrynie. To narzędzie jest udostępniane za pośrednictwem adresu URL HTTPS, aby zapewnić, że tekst nie zostanie skradziony.

W przypadku szyfrowania możesz wprowadzić zwykły tekst, hasło, plik obrazu lub plik .txt, który chcesz zaszyfrować. Teraz wybierz tryb szyfrowania blokowego. ECB (elektroniczna książka kodów) to najprostszy tryb szyfrowania i nie wymaga IV do szyfrowania. Wejściowy zwykły tekst zostanie podzielony na bloki, a każdy blok zostanie zaszyfrowany dostarczonym kluczem, a zatem identyczne bloki zwykłego tekstu są zaszyfrowane w identyczne bloki tekstu zaszyfrowanego. Tryb CBC jest wysoce zalecany i wymaga IV, aby każda wiadomość była unikalna.

Algorytm AES ma 128-bitowy rozmiar bloku, niezależnie od tego, czy długość klucza wynosi 256, 192 czy 128 bitów. Gdy tryb szyfrowania symetrycznego wymaga IV, długość IV musi być równa rozmiarowi bloku szyfru. Dlatego zawsze musisz używać IV 128 bitów (16 bajtów) z AES.

AES zapewnia 128-bitowy, 192-bitowy i 256-bitowy rozmiar tajnego klucza do szyfrowania. Należy pamiętać, że jeśli wybierasz 128 bitów do szyfrowania, tajny klucz musi mieć długość 16 bitów oraz 24 i 32 bity dla 192 i 256 bitów klucza. Teraz możesz odpowiednio wprowadzić tajny klucz. Domyślnie zaszyfrowany tekst będzie zakodowany w base64, ale masz również opcje wyboru formatu wyjściowego jako HEX.

Podobnie dla obrazu i pliku .txt zaszyfrowany formularz będzie zakodowany w Base64.

Więcej informacji na temat szyfrowania AES, odwiedź wyjaśnienie dotyczące szyfrowania AES.

Część 2. Jak odszyfrować plik bez hasła/klucza/certyfikatu offline (wykonaj notatkę)

Możesz odszyfrować system plików, odznaczając opcję „Zaszyfruj zawartość, aby zabezpieczyć dane". Ale działa to tylko dla systemu plików, a nie dla twojego konkretnego pliku. Jeśli chcesz odszyfrować pliki, niezbędny jest certyfikat lub hasło.

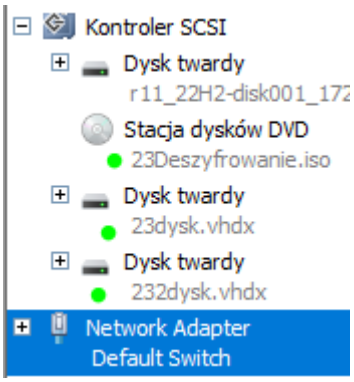
Jeśli nie wyeksportowałeś i nie utworzyłeś kopii zapasowej certyfikatu szyfrowania plików wcześniej lub jeśli zapomniałeś hasła, nie możesz odszyfrować zaszyfrowanych plików, jeśli wykonałeś jedną z następujących czynności:

1. Ponowna instalacja systemu operacyjnego Windows
2. Przenoszenie zaszyfrowanych plików na inny komputer
3. Odzyskiwanie danych z zaszyfrowanego dysku

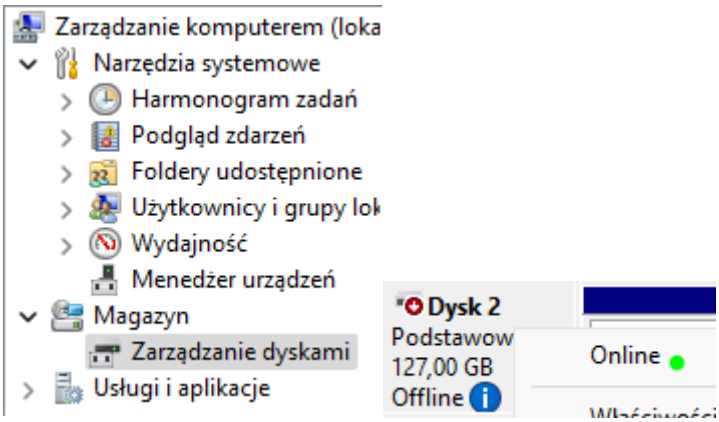
Część 3. Jak odzyskać zaszyfrowane pliki zablokowane przez oprogramowanie ransomware

Jeśli użytkownicy aktywnie używają narzędzi do szyfrowania, istnieje inny sposób szyfrowania plików, który polega na użyciu wirusów lub oprogramowania ransomware. Na przykład oprogramowanie ransomware szyfruje i usuwa pliki. W następnej części pokaże, jak korzystać z niezawodnego narzędzia do odzyskiwania zaszyfrowanych plików ransomware, aby odzyskać dane bez płacenia okupu.

Pobierz z materiałów i podłącz dodatkowo pliki dysków 23dysk.vhdx oraz 23Deszyfrowanie.iso



Upewnij się, że Network Adapter ustawiony jest jak na rysunku.



Ponieważ większość ransomware szyfruje twoje pliki i foldery w trzech krokach: utwórz dokładną kopię plików i folderów > zaszyfruj kopię > usuń pliki źródłowe. Sposób, w jaki to działa, daje świetną okazję do odzyskania zaszyfrowanych plików za pomocą profesjonalnego oprogramowania do odzyskiwania danych.

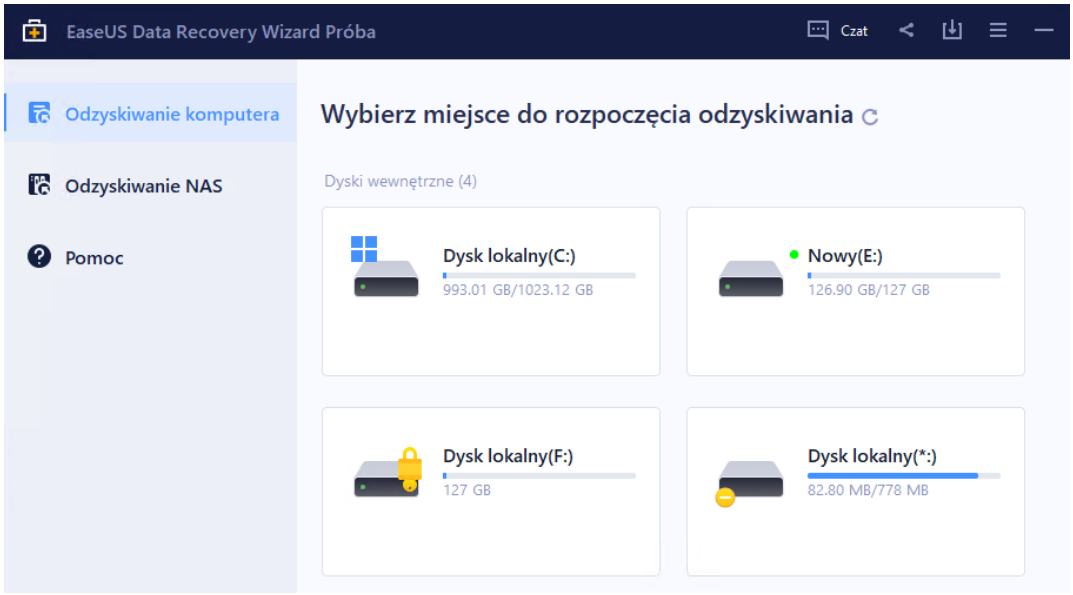
Wypróbuj dostępny na CD/DVD lub Internetu Kreatora odzyskiwania danych EaseUS. Ten program do odzyskiwania danych z ataków wirusów umożliwia odzyskanie plików zainfekowanych wirusem skrótów, przywrócenie plików usuniętych i zaszyfrowanych przez oprogramowanie ransomware, takie jak Locky, CryptoLocker, CryptoWall i TorrentLocker, bez płacenia.

Zainstaluj z DVD lub Internetu to narzędzie do odzyskiwania danych i zacznij odzyskiwać zaszyfrowane pliki ransomware w trzech krokach. Zauważ, że jest to tylko do odzyskiwania plików skrótów wirusowych lub ransomware, nie wliczając tych za pomocą narzędzi szyfrujących.

Krok 1. Wybierz zainfekowany wirusem dysk do skanowania [Nowy (E:)]

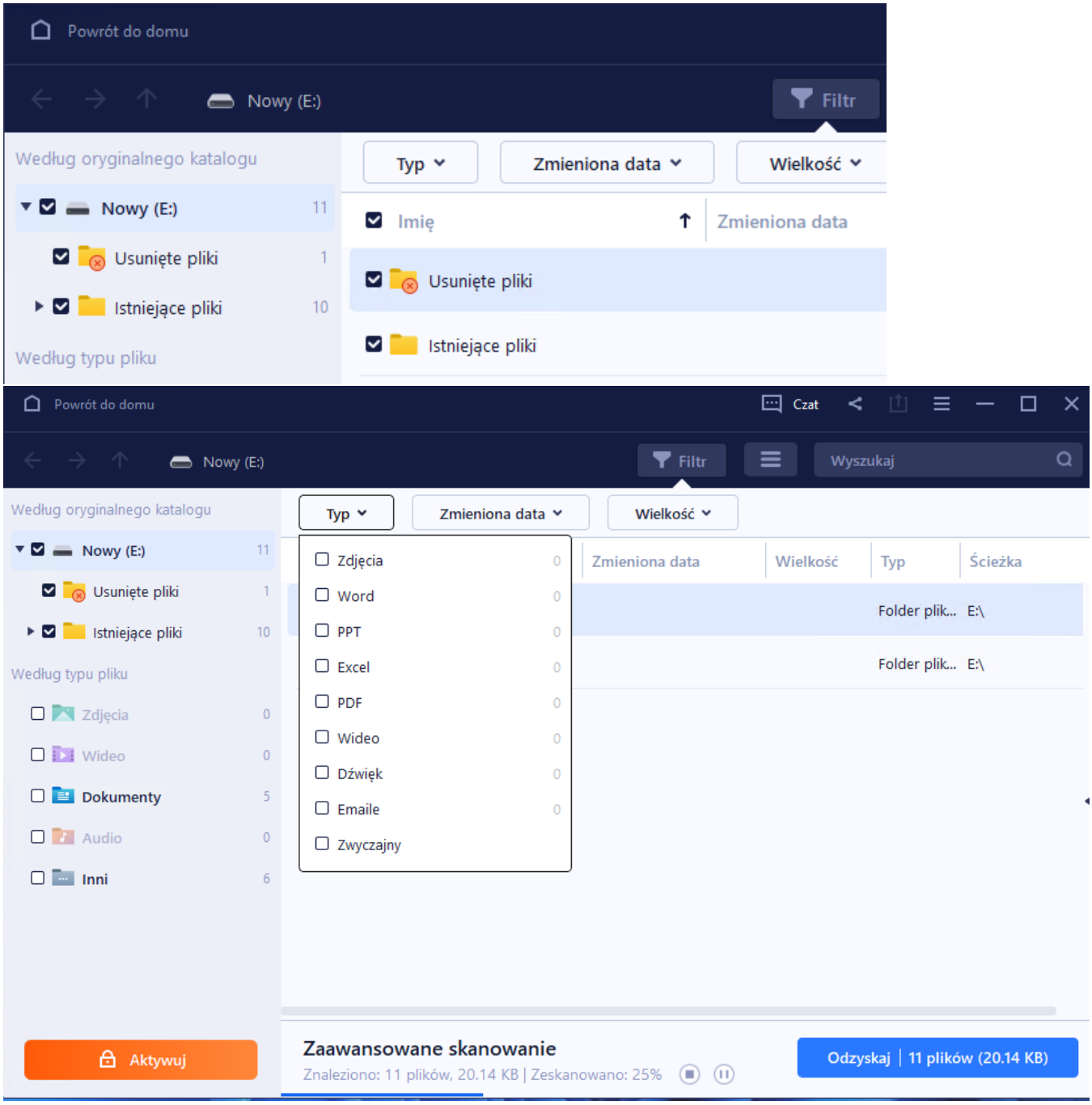
Uruchom oprogramowanie do odzyskiwania plików wirusów EaseUS na komputerze z systemem Windows. Wybierz dysk zaatakowany przez wirusa do skanowania w poszukiwaniu zagubionych lub ukrytych plików. Zwróć uwagę, że:

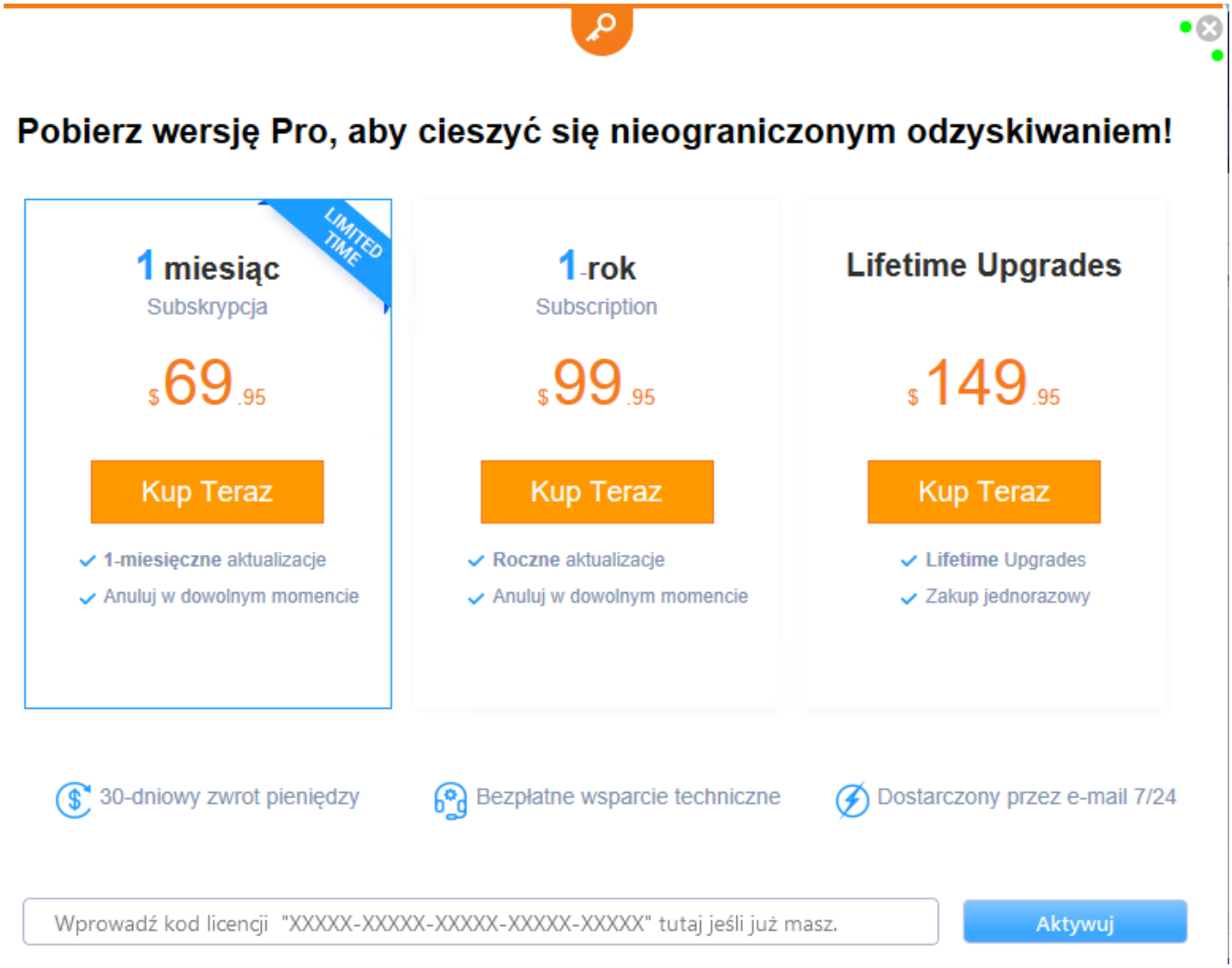
1. Jeśli jest to dysk twardy, na którym pliki zostały ukryte lub usunięte przez wirusa, lepiej zainstalować oprogramowanie na innym woluminie lub zewnętrznym dysku USB, aby uniknąć nadpisywania danych.
2. Jeśli zainfekowanym urządzeniem jest zewnętrzny dysk twardy, pendrive lub karta pamięci, nie ma znaczenia czy oprogramowanie zostanie zainstalowane na lokalnym dysku komputera.



Krok 2. Sprawdź wszystkie zeskanowane wyniki

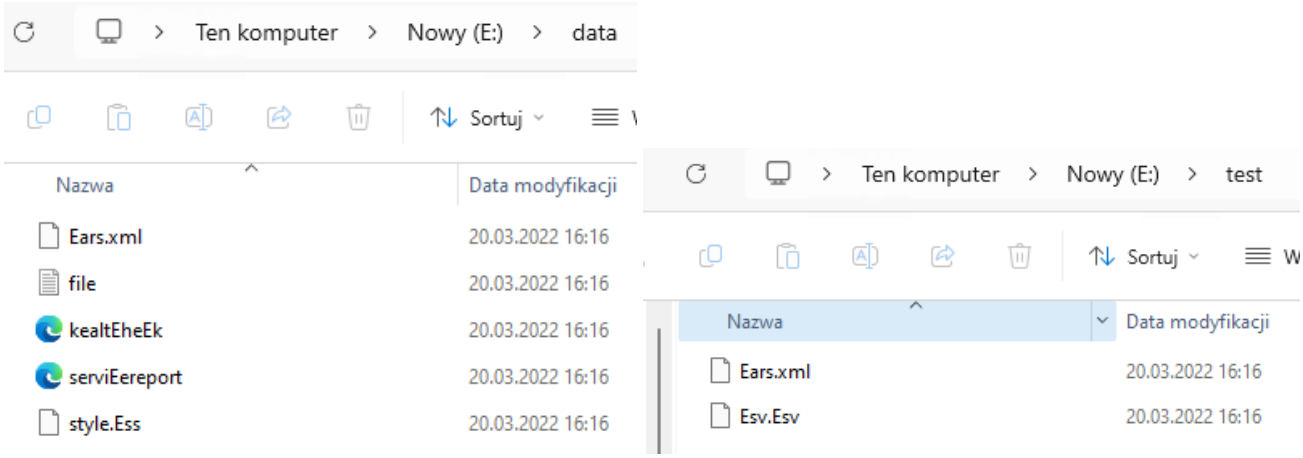
Kreator odzyskiwania danych EaseUS natychmiast rozpocznie proces skanowania, aby znaleźć usunięte lub ukryte pliki na dysku twardym zainfekowanym wirusem. Aby szybko zlokalizować żądane pliki, możesz użyć funkcji filtrowania lub grupowania typów, aby wyświetlić tylko zdjęcia, filmy, dokumenty, e-maile itp.


Powrót do domu
Nowy (E:)
Filtr
Według oryginalnego katalogu
Nowy (E:) 11
Usunięte pliki 1
Istniejące pliki 10
Według typu pliku
Typ
Zmieniona data
Wielkość
Imię
Zmieniona data
Usunięte pliki
Istniejące pliki
Powrót do domu
Czat
Nowy (E:)
Filtr
Wyszukaj
Według oryginalnego katalogu
Nowy (E:) 11
Usunięte pliki 1
Istniejące pliki 10
Według typu pliku
Zdjęcia 0
Wideo 0
Dokumenty 5
Audio 0
Inni 6
Typ
Zmieniona data
Wielkość
Zdjęcia 0
Word 0
PPT 0
Excel 0
PDF 0
Wideo 0
Dźwięk 0
Emaile 0
Zwyczajny 0
Zmieniona data
Wielkość
Typ
Ścieżka
Folder plik... E:\
Folder plik... E:\
Aktywuj
Zaawansowane skanowanie
Znaleziono: 11 plików, 20.14 KB | Zeskanowano: 25%
Odzyskaj | 11 plików (20.14 KB)



Krok 3. Wyświetl podgląd i odzyskaj usunięte/ukryte pliki

Po zakończeniu procesu możesz wyświetlić podgląd zeskanowanych plików. Wybierz żądane pliki i kliknij przycisk „Odzyskaj”. Przywrócone pliki należy zapisywać w innej bezpiecznej lokalizacji na komputerze lub urządzeniu pamięci masowej, a nie tam, gdzie zostały utracone.



Pokaż efekty