Encrypted Disk 3.0

Podręcznik użytkownika

Spis treści

O programie Encrypted Disk.....3
Składniki pakietu.....3
Minimalne wymagania systemowe.....3
Podstawowa koncepcja kryptografii.....4
Omówienie interfejsu.....5
Używanie paska zadań Windows.....5
Używanie eksploratora Windows.....6
Menadżer Encrypted Disk.....8
Układ ogólny.....9
Explorer bar.....9
Encrypted disks list 10
Tool bar.....10
Main menu.....11
Utilities bar.....12
Status bar.....13
Zarządzanie dyskiem zaszyfrowanym.....13
Tworzenie dysków zaszyfrowanych 13
Ponowne szyfrowanie dysków.....18
Wyszukiwanie dysków zaszyfrowanych 21
Dodawanie dysków zaszyfrowanych.....22
Montowanie dysków zaszyfrowanych.....23
Montowanie za pomocą paska zadań Windows System Tray.....23
Montowanie za pomocą eksploratora Windows.....24
Montowanie za pomocą menadżera Encrypted Disk Manager.....24
Odmontowanie dysków zaszyfrowanych.....25
Odmontowanie za pomocą paska zadań Windows System.....26
Odmontowanie za pomocą eksploratora Windows.....26
Odmontowanie za pomocą menadżera Encrypted Disk Manager.....26
Formatowanie dysków zaszyfrowanych.....27
Przeglądanie właściwości dysku zaszyfrowanego.....27
Właściwości dysku zaszyfrowanego w eksploratorze Windows 28
Właściwości dysku zaszyfrowanego w menadżerze ED Manager.....29
Udostępnianie dysków zaszyfrowanych.....32
Usuwanie dysków zaszyfrowanych.....32

O programie Encrypted Disk

Encrypted Disk to zestaw sterowników systemowych, plug-inów, kreatorów i narzędzi do przechowywania danych w formie zaszyfrowanej, ale używania ich w standardowy sposób, tak jakby nie były zaszyfrowane. Oprogramowanie to przeznaczone jest dla tych użytkowników, którzy chcą zaszyfrować ważne informacje, ale nie mają wystarczająco dużo czasu, aby uczyć się kryptografii.

Program posiada następujące główne funkcje:

• Szyfrowanie/odszyfrowywanie „w locie” wszystkich operacji, niezauważalnie dla użytkownika.

• Ponowne szyfrowanie bez konieczności przenoszenia danych.

• Ochrona hasłem lub kluczem zewnętrznym, który można umieścić na nośniku wymiennym.

• Umieszczenie zaszyfrowanych plików kontenera dysku (pliki obrazu), gdziekolwiek użytkownik zechce: na dyskach twardych, dyskach sieciowych lub nośnikach wymiennych.

Program został zaprojektowany na bazie Encrypted Disk SDK, który jest odrębnym oprogramowaniem, przeznaczonym dla aplikacji Windows.

Składniki pakietu

Pakiet instalacyjny programu zawiera:

• Sterowniki systemowe i plug-iny szyfrowania.

• Plug-iny do eksploratora Windows (rozszerzenia powłoki Windows).

• Menu paska zadań Windows.

• Kreator tworzenia (New Encrypted Disk Wizard).

• Kreator ponownego szyfrowania (Re-encryption Wizard).

• Menadżer Encrypted Disk Manager.

Minimalne wymagania systemowe

Aby używać programu na komputerze, upewnij się, że system spełnia minimalne wymagania systemowe:

• Systemy operacyjne: Windows 98/Me/2000/XP/Server 2003

• Procesor Intel Pentium lub inny odpowiadający mu procesor 300 MHz

• 64 MB RAM

• Wolne miejsce na dysku twardym: 12MB

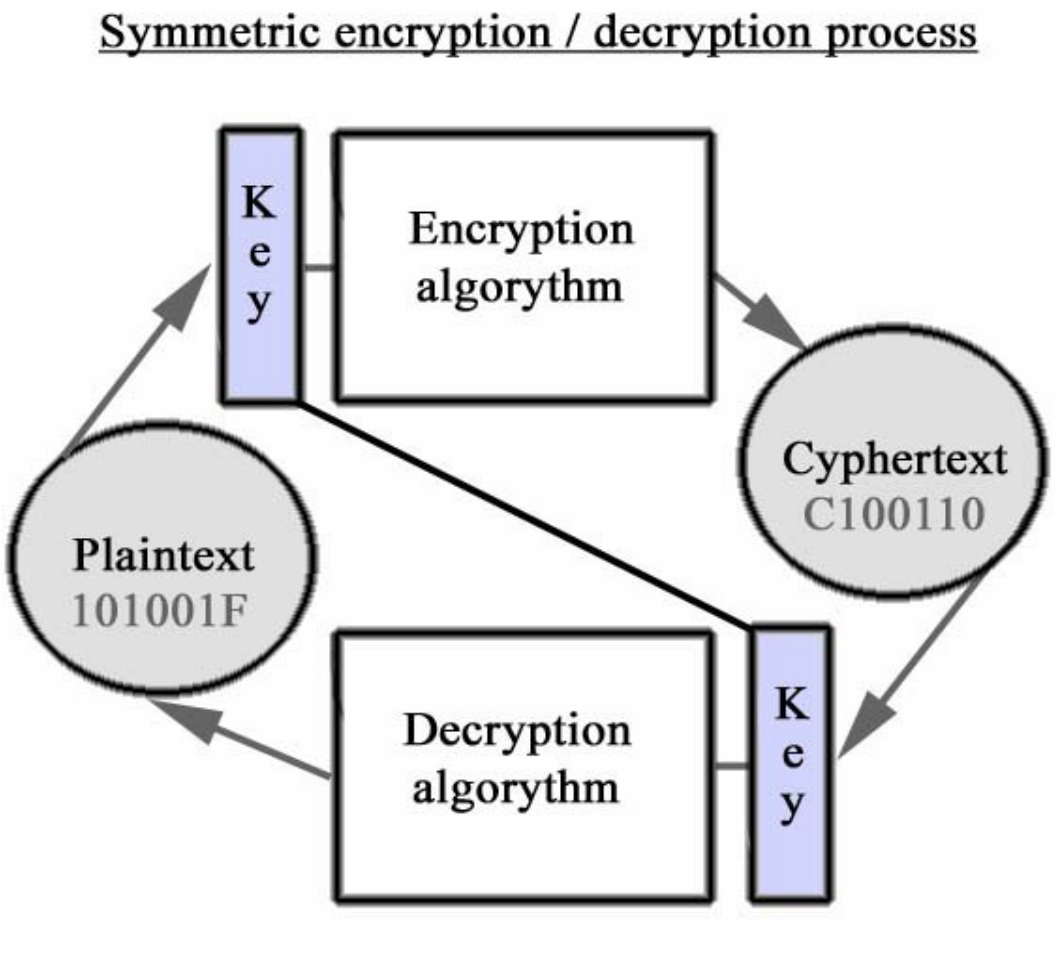
• Karta graficzna SVGA i monitor

• Mysz

Podstawowa koncepcja kryptografii

Szyfrowanie jest zrozumiałym procesem konwertowania danych w szyfr, który można odkodować do jego oryginalnej formy. Zestaw zasad dla takiej konwersji wyrażony jest w postaci algorytmu. Niektóre podstawowe algorytmy mogą być połączone, aby utworzyć bardziej skomplikowane. Na przykład podstawowe algorytmy mogą zmieniać kolejność indywidualnych symboli lub zastępować symbole innymi symbolami.

Szyfr, który produkowany jest poprzez jednoczesną konwersję grupy zrozumiałych danych w grupę szyfru, nazywany jest blokiem szyfru. W zasadzie, grupy mają ten sam rozmiar. Aby zaszyfrować dane algorytm szyfru używa tak zwanego klucza szyfrowania. Klucz szyfrowania to sekwencja wartości, wybranych przypadkowo. Typ i długość tej sekwencji zależy od algorytmu szyfrowania i sumy potrzebnych zabezpieczeń. Jeśli użytkownik może szyfrować i odszyfrowywać dane za pomocą jednego klucza, taki algorytm szyfru nazywany jest symetrycznym. W przypadku algorytmów asymetrycznych, klucz szyfrowania różni się od klucza odszyfrowywania. Jeden jest kluczem publicznym, za pomocą którego nadawca może szyfrować tekst, a inny jest kluczem prywatnym, za pomocą odbiorca może odszyfrować tekst.



Najpopularniejsze algorytmy symetryczne to:

DES (Data Encryption Standard). Algorytm ten został opracowany przez firmę IBM Corporation i jest używany na całym świecie od roku 1977. Pracuje on z 64-bitowymi blokami danych. Długość klucza wynosi 62 bity, ale 8 bitów może zostać użyte do wykrycia błędów, więc prawdziwa długość klucza to 56 bitów. Obecnie algorytm ten jest przestarzały, ponieważ długość kluczy nie jest wystarczająca, żeby chronić dane przed złamaniem przez testowane klucze.

Triple DES. Jest to ulepszona wersja DES. Podczas procesu szyfrowania używa trzykrotnie algorytmu DES, i za

każdym razem wprowadzony zostaje inny klucz. Algorytm ten jest bezpieczniejszy niż DES.

Blowfish. Algorytm został zaprojektowany w 1993 roku przez Bruce Schneier, jako szybsza i darmowa alternatywa dla istniejących algorytmów szyfrowania. Od tego czasu powoli zdobywał zaufanie, jako mocny algorytm szyfrowania. Pracuje z 64 bitowymi blokami danych. Charakterystyczną właściwością algorytmu jest zmienna długość klucza, która wynosi od 32 bitów do 448. Podczas generowania klucza algorytm używa 521 cyklów szyfrowania, co poważnie utrudnia złamanie przez klucze testowane. Blowfish pracuje znacznie szybciej niż DES.

AES (Advanced Encryption Standard). Algorytm zaprojektowany jako nowe standardy rządowe Stanów Zjednoczonych (zamiast DES). Pracuje z 128, 192 i 256 bitowymi blokami danych i używa kluczy szyfrowania o długości 128, 192 i 256 bitowych (istnieje 9 możliwych kombinacji).

Omówienie interfejsu

Większość operacji na dyskach zaszyfrowanych można wykonać za pomocą paska zadań Windows lub eksploratora Windows. Program używa w tym celu specjalnych sterowników i plug-inów. Jeśli użytkownik posiada znaczną ilość dysków zaszyfrowanych, może je w wygodny sposób uporządkować za pomocą specjalnego narzędzia zwanego menadżerem Encrypted Disk Manager.

Używanie paska zadań Windows

Podczas instalacji program dodaje swoją ikonę w pasku zadań Windows. Poprzez kliknięcie na nią prawym przyciskiem myszy użytkownik może otworzyć menu, które zapewnia dostęp do wszystkich potrzebnych funkcji programu.

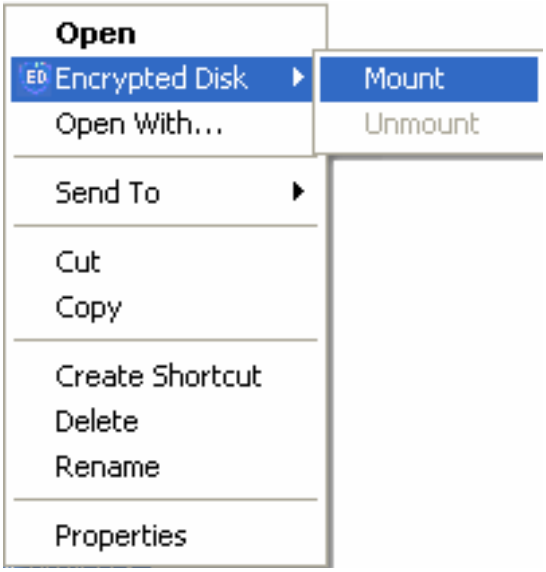
Elementy menu podzielone są na cztery sektory:

Wizards starting	
Encrypted Disk Manager	Zarządzanie istniejącymi dyskami zaszyfrowanymi
New Encrypted Disk Wizard	Utworzenie nowego dysku zaszyfrowanego
Re-encryption Wizard	Ponowne szyfrowanie istniejącego dysku zaszyfrowanego lub zmiana jego klucza.
Encrypted disks management	

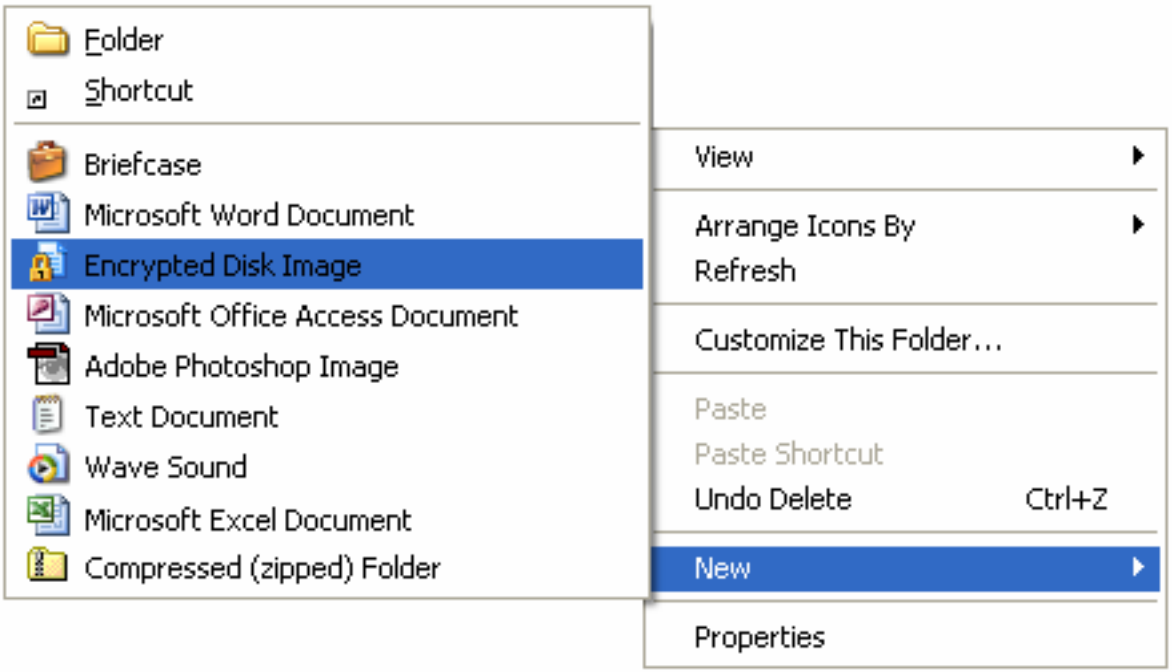
Mount	Montowanie jednego z zaszyfrowanych dysków
Disks	Dostęp do listy zaszyfrowanych dysków i operacji na nich (otworzenie, odmontowanie).
Help	
Help	Otworzenie tego podręcznika
About	Uruchomienie okna z informacją o programie.
Exit	
Exit	Wyjście z programu. Ikona programu zniknie z paska zadań Windows.

Używanie eksploratora Windows

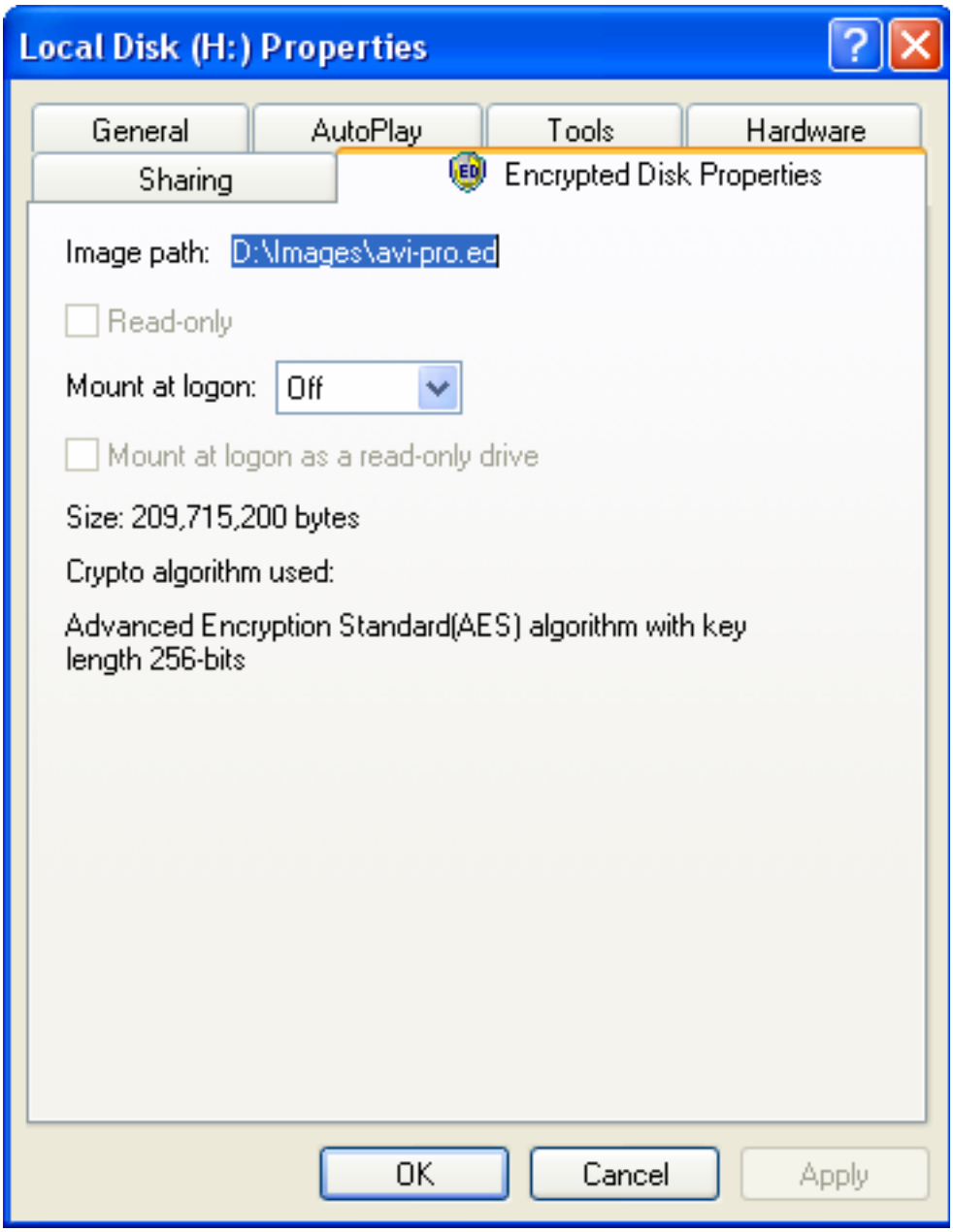
Podczas instalacji program dodaje nowy element Encrypted Disk w sekcji **File** w menu głównym eksploratora Windows i w tej samej sekcji menu kontekstowego (jeśli wybrany zostanie zaszyfrowany dysk lub plik obrazu). Menu to pozwala na montowanie lub odmontowanie wybranego dysku zaszyfrowanego.



Sterowniki programu pozwalają również na tworzenie nowego dysku zaszyfrowanego poprzez sekcję **New** w menu kontekstowym eksploratora Windows. To podmenu służy do tworzenia nowych plików zarejestrowanego oprogramowania. Po wybraniu elementu **Encrypted Disk Image** pojawia się kreator **New Encrypted Disk Wizard**.



Okno **File / Disk Properties** będzie miało dodatkowy element – **Encrypted Disk Properties**, który zawiera informacje o wybranym dysku zaszyfrowanym lub pliku obrazu (plik, który zawiera dane dysku zaszyfrowanego). Zobacz rozdział Przeglądanie właściwości dysku zaszyfrowanego, aby dowiedzieć się więcej.



Menadżer Encrypted Disk

Encrypted Disk Manager to specjalne narzędzie do zarządzania dyskami zaszyfrowanymi. Można uzyskać do niego dostęp poprzez:

• Menu **Start**:

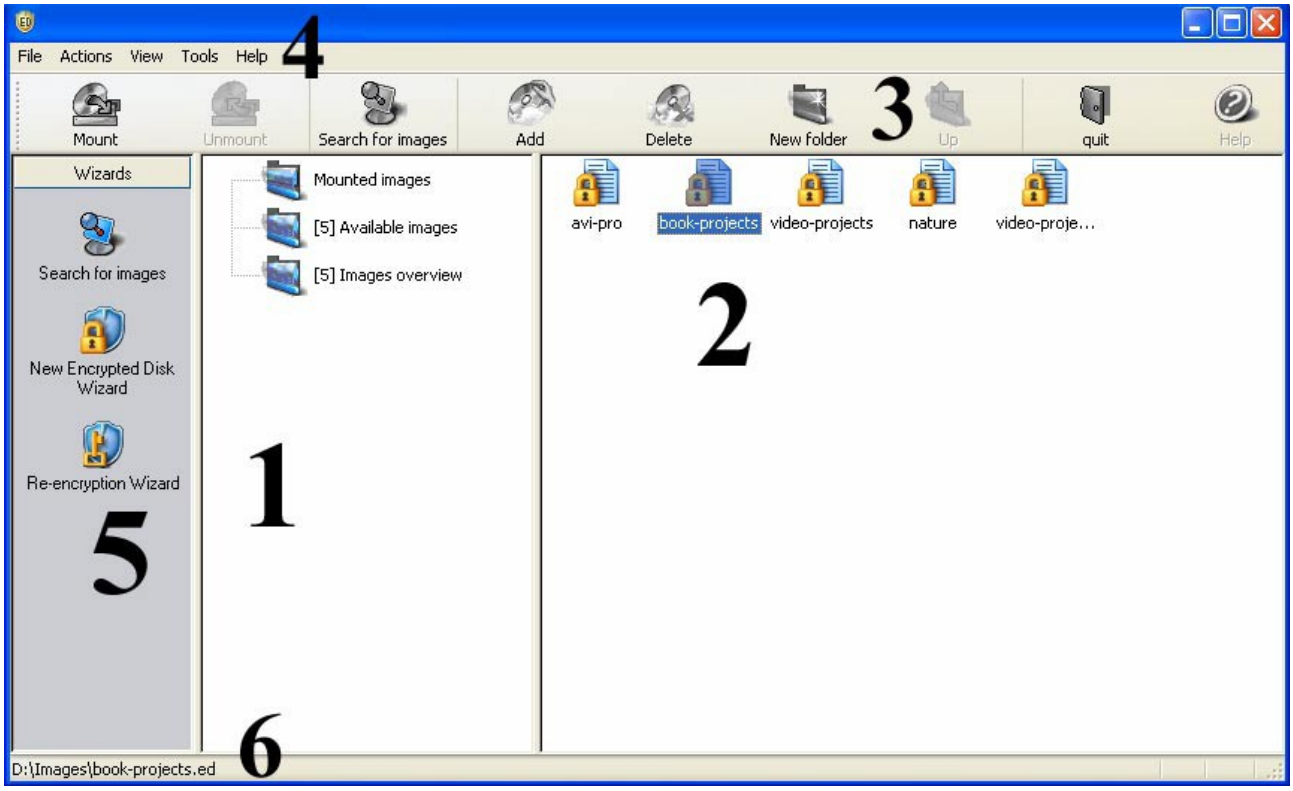
Programs > …Encrypted Disk > Encrypted Disk Manager

• Pasek zadań Windows:

Element **Encrypted Disk Manager** w menu **Encrypted Disk**.

Układ ogólny

Menu główne programu podzielone jest na kilka części, które służą różnym celom:



1. Explorer bar

2. Encrypted disks list

3. Tool bar

4. Main menu

5. Utilities bar

6. Status bar

Explorer bar

Pasek Explorer bar służy do porządkowania i wyświetlania zawartości lokalnej bazy danych obrazów zaszyfrowanego dysku w formie hierarchicznej oraz szybkiego zarządzania dyskami zaszyfrowanymi. W bazie danych obrazów zaszyfrowanych dysków, wszystkie obrazy posortowane są w kilka kategorii, które wyświetlone są jako foldery bazy danych. Użytkownik może manipulować obrazami umieszczonymi w bazie danych:

• Tworzenie nowych folderów i podfolderów

• Zmiana nazwy folderów (za wyjątkiem domyślnych)

• Usuwanie folderów (za wyjątkiem domyślnych)

Użytkownik może używać wszystkich tych funkcji w specjalnym folderze bazy danych, zwanym **Available**

Images.

Pasek Explorer bar wyświetla dwa specjalne foldery, które mają następujące właściwości:

• Specjalny folder o nazwie **Images Overview** zapewnia pełną listę wszystkich obrazów znajdujących się w bazie danych, dla szybkiego wyszukania zagubionych obrazów. W folderze tym nie można utworzyć podfolderów ani przenosić obrazów.

• Folder o nazwie **Mounted Images** wyświetla listę wszystkich obrazów dysków zaszyfrowanych, które zamontowane są w systemie. Program dodaje automatycznie nowo zamontowane obrazy. W folderze tym również nie można tworzyć podfolderów.

Encrypted disks list

Lista Encrypted disk ulokowana jest w prawej części okna głównego. Wyświetla obrazy zaszyfrowanych dysków znajdujących się w folderze wybranym w pasku Explorer bar. Użytkownik może manipulować obrazami w następujący sposób:

• Dowolnie przenosić obrazy pomiędzy folderami

• Tworzyć nowe foldery i podfoldery

• Zmieniać nazwy folderów (za wyjątkiem domyślnych)

• Zmieniać nazwy obrazów

• Usuwać foldery (za wyjątkiem domyślnych)

Tool bar

Pasek Tool bar zapewnia szybki dostęp do najczęściej używanych operacji:

Przycisk	Funkcjonalność
	Montowanie wybranego dysku zaszyfrowanego
	Odmontowanie wybranego dysku zaszyfrowanego
	Wyszukiwanie obrazów dysków zaszyfrowanych

	Dodanie obrazu dysku zaszyfrowanego do bieżącego folderu
	Usunięcie obrazu dysku zaszyfrowanego z bieżącego folderu
	Dodanie nowego podfolderu do bieżącego folderu
	Przeniesienie do wyższego poziomu foldera
	Wyjście z programu

Main menu

Main menu zapewnia jednolity dostęp do pełnej funkcjonalności programu.

File	
New	
Folder	Tworzenie nowego podfolderu w folderze. Dostępne jedynie jeśli jakiś folder został wybrany w oknie Menadżera
Add Image	Ręczne dodanie obrazu dysku zaszyfrowanego, który nie znajduje się w bazie danych do tego folderu. Element ten nie aktywuje kreatora Find images Wizard
Delete	Usunięcie obrazu z bazy danych (z możliwością usunięcia plików obrazu z dysku).
Rename	Zmiana etykiety obrazu dysku zaszyfrowanego, która reprezentuje obraz w bazie danych.
Change Icon	Zmiana piktogramu, który reprezentuje obrazy dysków w bazie danych
Image properties	Wyświetlenie i edycja właściwości wybranego obrazu dysku.
Exit	Wyjście z menadżera Encrypted Disk Manager.

Actions	
Mount	Montowanie obrazu dysku zaszyfrowanego wybranego w liście Encrypted Disk List
Unmount	Odmontowanie obrazu dysku zaszyfrowanego wybranego w liście Encrypted Disk List
Unmount all	Odmontowanie wszystkich obrazów dysków zaszyfrowanych
View	
Utilities Bar	Wyświetlenie paska Utilities Bar po lewej stronie okna menadżera Encrypted Disk Manager
Toolbar	Wyświetlenie paska Toolbar w górnej części okna menadżera Encrypted Disk Manager
Status bar	Wyświetlenie paska Toolbar w dolnej części okna menadżera Encrypted Disk Manager
Big Icons	Użycie dużych piktogramów dla folderów i obrazów w bazie danych
Small Icons	Użycie małych piktogramów dla folderów i obrazów w bazie danych
List	Wyświetlenie listy, zawierającej foldery bazy danych (po jednym elemencie w linii)
Refresh	Ponowne przeskanowanie i wyświetlenie zawartości bazy danych obrazów.
Tools	
Search for images	Uruchomienie kreatora Find Wizard, który pozwala na wyszukanie obrazów dysków zaszyfrowanych nie wyświetlonych w bazie danych.
New Encrypted Disk Images	Utworzenie nowego obrazu dysku zaszyfrowanego
Re-encrypt Encrypted Disk Image	Ponowne szyfrowanie istniejącego obrazu dysku zaszyfrowanego
Help	
Index	Wyświetlenie zawartości pomocy
About…	Wyświetlenie okna dialogowego z informacją o programie

Utilities bar

Pasek Utilities toolbar ulokowany jest w lewej części okna głównego. Służy on do szybkiego uruchamiania kreatorów programu:

Przycisk	Funkcjonalność
	Wyszukanie obrazów dysków zaszyfrowanych

	Utworzenie nowego dysku zaszyfrowanego
	Ponowne szyfrowanie istniejącego dysku zaszyfrowanego

Status bar

To najniższa część okna głównego. Pasek status bar wyświetla kilka dodatkowych informacji – menu wskazówek (krótki opis), pełną ścieżkę wybranego pliku obrazu.

Zarządzanie dyskiem zaszyfrowanym

Głównym celem programu jest tworzenie i zarządzanie dyskami zaszyfrowanymi. Program tworzy pliki obrazów dysków zaszyfrowanych, które mogą być przedstawione w formie normalnej litery dysku. Jest to niezauważalne dla użytkownika i aplikacji, które uruchamiają i ładują pliki z dysku zaszyfrowanego. Fizycznie pliki obrazów dysków zaszyfrowanych mogą być przechowywane na dyskach lokalnych lub sieciowych. W przypadku dysków sieciowych, szyfrowanie daje użytkownikowi dodatkową ochronę. Nawet jeśli standardowe narzędzia ochrony sieciowej zostaną złamane, pliki obrazów pozostaną zaszyfrowane i nie będzie możliwy do nich dostęp bez odpowiedniego klucza. Rozdział ten opisuje operacje, jakie użytkownik może wykonać na dyskach zaszyfrowanych.

Tworzenie dysków zaszyfrowanych

Tworzenie nowych dysków zaszyfrowanych realizowane jest za pomocą kreatora **New Encrypted Disk Wizard.** Można go uruchomić na trzy sposoby:

• Za pomocą paska zadań Windows:

1. Kliknij prawym przyciskiem myszy na ikonę dysku zaszyfrowanego w pasku zadań.

2. Wybierz element **New Encrypted Disk Wizard** w menu.

• Za pomocą pulpitu Windows :

1. Kliknij prawym przyciskiem myszy na pulpit Windows.

2. Wybierz element **New** item w menu kontekstowym.

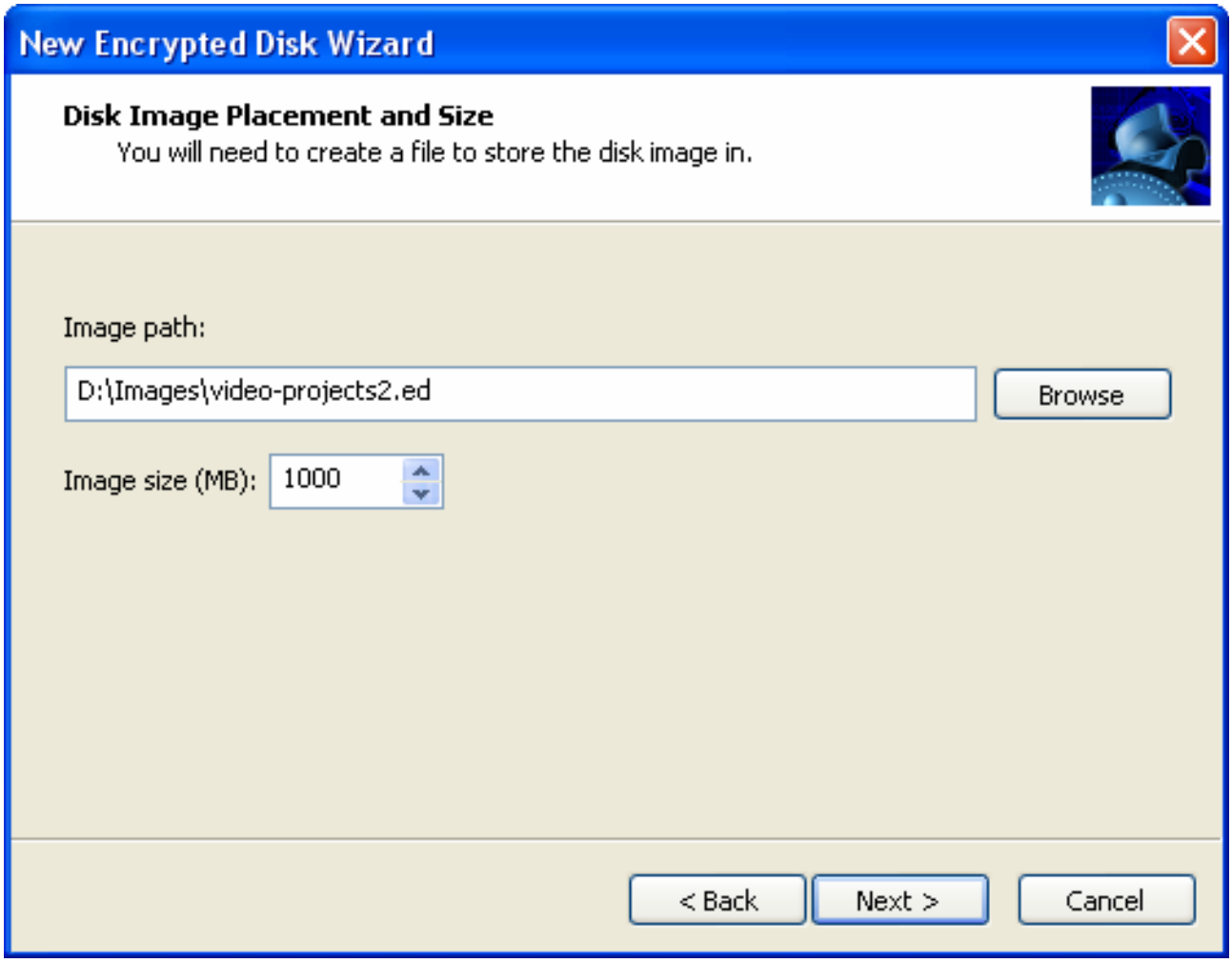
3. Wybierz element **Encrypted Disk Image**.

• Za pomocą menadżera Encrypted Disk Manager:

Kliknij przycisk **New Encrypted Disk Wizard** w pasku Utilities bar.

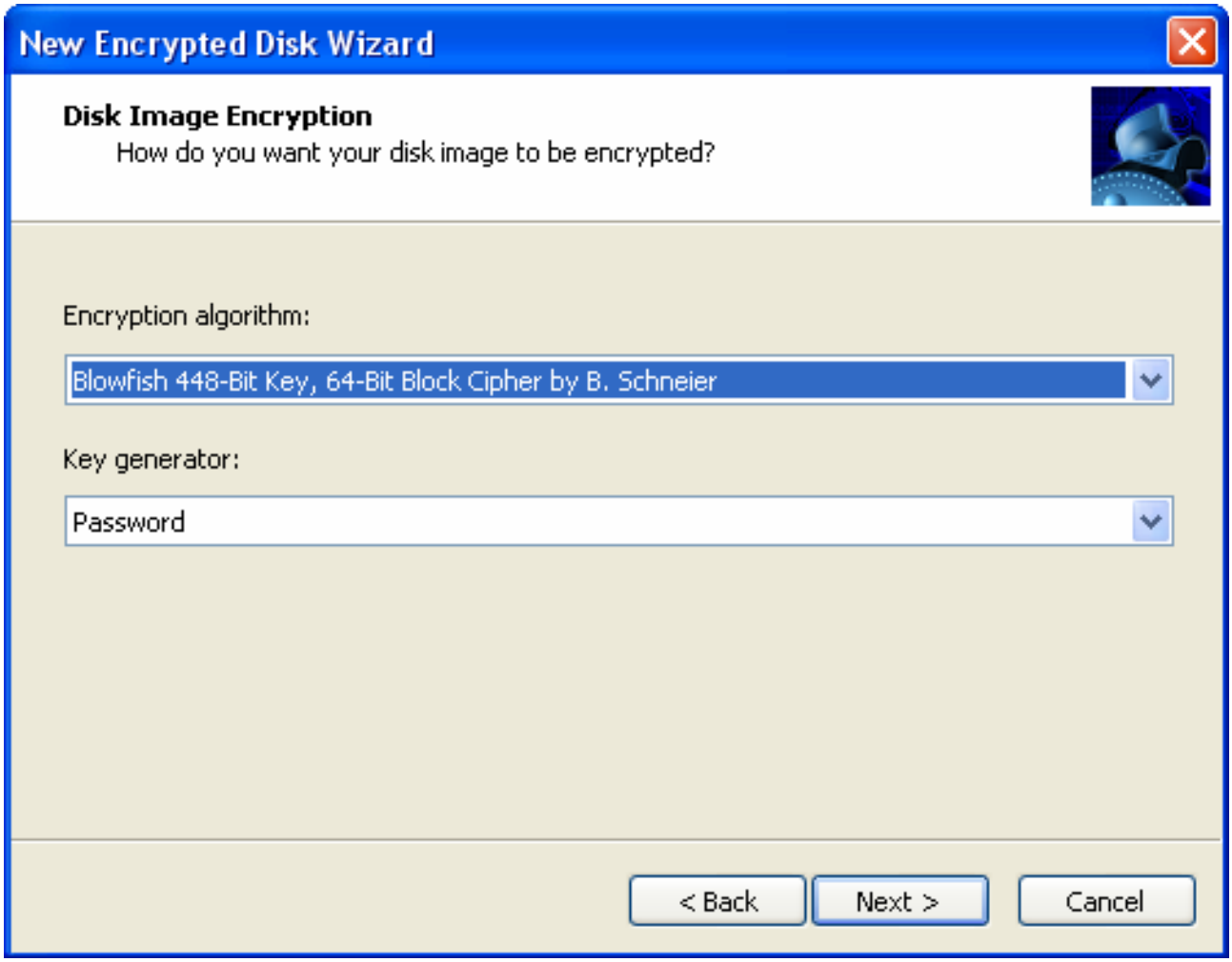
Pierwsza strona kreatora (Strona **Welcome**) informuje użytkownika o funkcjach operacji. Przeczytaj ją dokładnie i kliknij przycisk **Next**, aby kontynuować.

Druga strona (Strona **Disk Image Placement and Size**) proponuje określenie miejsca i rozmiaru pliku, który zawierać będzie nowy dysk zaszyfrowany. Pliki takie nazywane są obrazami.



Użytkownik może podać pełną ścieżkę do przyszłego pliku obrazu na dysku twardym lub użyć do tego celu standardowego przeglądania plików. Aby rozpocząć przeglądanie plików, kliknij przycisk **Browse.** Pliki obrazów dysków zaszyfrowanych mają rozszerzenie - ***.ed**. Rozmiar nowego pliku wskazany jest w polu **Image size** znajdującym się pod polem **Image.** Użyj suwaków po prawej stronie pola aby poprawić wartość. Po określeniu parametrów pliku obrazu, kliknij przycisk **Next**, aby kontynuować.

Trzecia strona (strona **Disk Image Encryption Page**) pozwala określić parametry szyfrowania dla szyfrowanego dysku. Użytkownik powinien ustawić algorytm szyfrowania i metodę generowania klucza. Metoda generowania klucza określa czy klucz szyfrowania będzie generowany w oparciu o podane hasło czy w oparciu o dowolne zdarzenie systemowe (element **Key from file**). W ostatnim przypadku klucz będzie przechowywany w osobnym pliku na nośniku zewnętrznym.



Program zapewnia następujące algorytmy szyfrowania, które użytkownik może wybrać w menu **Encryption algorithm**:

• Advanced Encryption Standard (AES) algorytm z kluczem o długości 256-bitów;

• Blowfish z kluczem 448-Bitowym, 64-Bitowy Block Cipher B.Schneier'a;

• DES (Date Encryption Standart) z kluczem o długości 56-bitów;

• Triple DES z kluczem o długości 168-bitów.

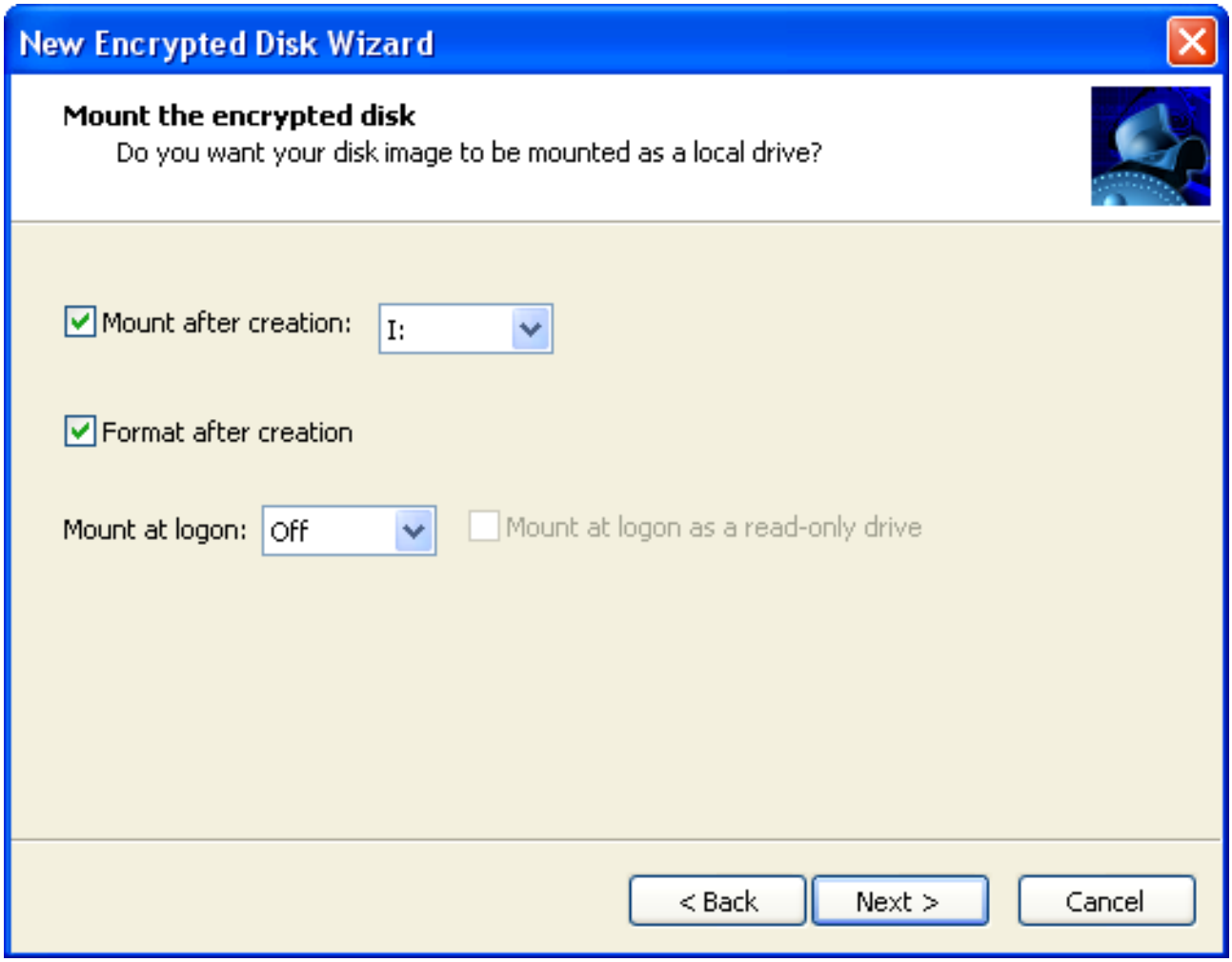
Przeczytaj rozdział Podstawowa koncepcja kryptografii, aby poznać szczegóły na temat algorytmów.

Wybrany algorytm użyje specjalnej sekwencji wartości – klucz do szyfrowania lub odszyfrowania danych. Klucz generowany jest w trakcie tworzenia pliku obrazu dysku zaszyfrowanego. Następnie przechowywany jest w osobnym pliku (plik powinien zostać umieszczony na nośniku wymiennym – dyskietce, dysku USB, itp.). Wybierz element **Key from file** w menu **Key generator** aby w ten sposób pracować z kluczem. Inne rozwiązanie wymaga podania hasła przez użytkownika i generowanie klucza odbędzie się w oparciu o to hasło. Wybierz element **Password** w menu.

Po podaniu parametrów szyfrowania kliknij **Next**, aby kontynuować.

Czwarta strona (strona **Mount the encrypted disk**) pozwala na zamontowanie nowego dysku zaszyfrowanego jako dysk lokalny. Nowy dysk zaszyfrowany można również zamontować później, po

utworzeniu.



Istnieją cztery opcje, które użytkownik może określić na tej stronie:

Mount after creation. Wybierz tę opcję, aby zamontować utworzony obraz dysku jako dysk lokalny i następnie przypisać do niego literę dysku. Lista dostępnych liter dysku znajduje się po prawej stronie.

Format after creation. Wybierz tę opcję, aby sformatować nowy dysk.

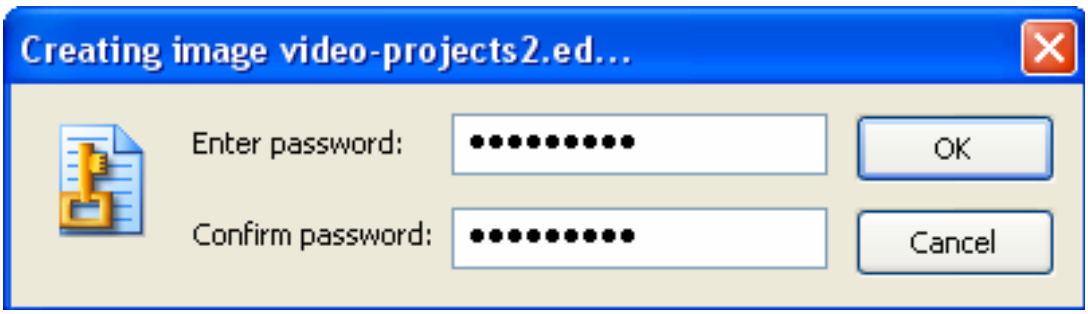
Mount at logon. Wybierz tę opcję, aby zamontować nowy dysk po każdym zalogowaniu się przez użytkownika. Menu rozwijane pozwala na wybranie litery dysku. Pole wyboru znajdujące się po prawej stronie pozwala na zamontowanie dysku tylko do odczytu.

Kliknij przycisk **Next** aby rozpocząć tworzenie nowego obrazu dysku zaszyfrowanego. Zajmie to około 2-3 minuty. W niektórych przypadkach w trakcie operacji potrzebne jest określenie dodatkowych parametrów:

Jeśli wartość **Key from file** została wybrana jako generator klucza(na stronie **Disk Image Encryption**) kreator zaproponuje określenie bezpiecznego miejsca do przechowywania klucza szyfrowania.

Zalecane jest przechowywanie go na nośniku wymiennym. Zwiększa to szanse na uniknięcie nieupoważnionego dostępu do danych.

Jeśli wartość **Password** została wybrana jako generator klucza (na stronie **Disk Image Encryption**), kreator zaproponuje podanie hasła i następnie potwierdzenie.



Istnieją pewne zasady, które pozwalają na wybranie wiarygodnego hasła. Na przykład:
- **Zalecane jest użycie długiego hasła, które zawiera litery i cyfry.**
- **Hasło powinno zawierać duże i małe litery.**
- **Należy unikać w haśle zwyczajnych słów.**

Jeśli wybrana została opcja **Format after creation** na stronie **Mount the encrypted disk**, kreator zaproponuje określenie parametrów formatowania, po wypełnieniu tego formularza dysk zostanie sformatowany.

Strona kreatora **The completing** informuje użytkownika o pomyślnym utworzeniu nowego dysku zaszyfrowanego i proponuje dodanie go do bazy danych menadżera Encrypted Disk Manager. Wybierz w tym celu pole wyboru **Add into Encrypted Disk Manager**. Jeśli określone zostały parametry montowania nowy dysk zaszyfrowany pojawi się w systemie z przypisaną literą dysku. Całkowita liczba dysków zaszyfrowanych, jakie można utworzyć i używać ograniczona jest jedynie przez dostępne miejsce.

Ponowne szyfrowanie dysków

Istnieje możliwość zmiany algorytmu szyfrowania istniejącego dysku. Kreator **Reencrypting Wizard** jest specjalnie przeznaczony do tego celu. Kreator pomoże również ustawić nowe hasło lub nowy klucz szyfrowania dla obrazu.

Użytkownik może uruchomić to narzędzie na dwa sposoby:

• Za pomocą paska zadań Windows:

1. Kliknij prawym przyciskiem myszy na ikonę **Encrypted Disk** w pasku zadań.

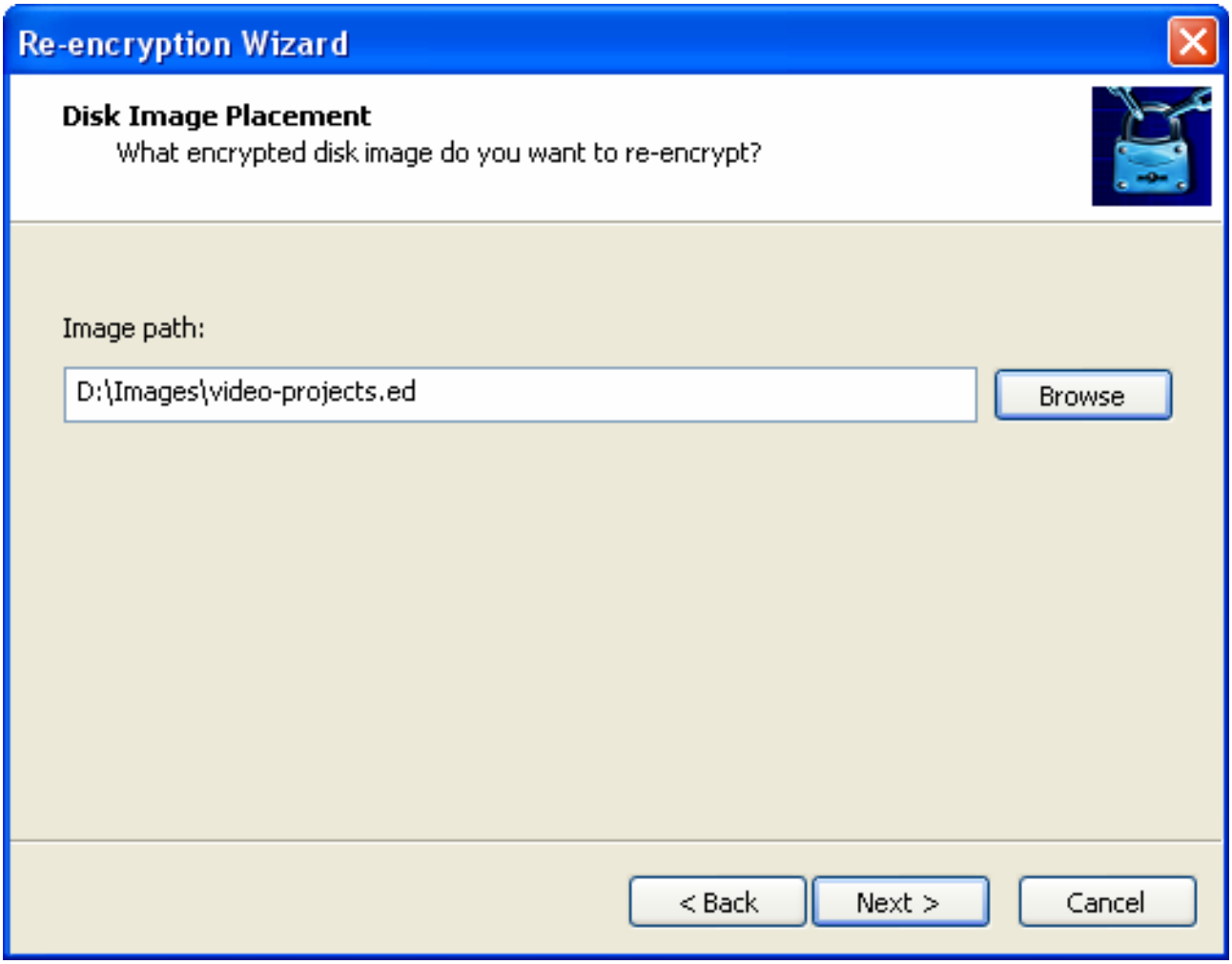
2. Wybierz z menu element **Re-encryption Wizard**.

• Za pomocą menadżera **Encrypted Disk Manager**:

Kliknij przycisk **Re-encryption Wizard** w pasku **Utilities bar**.

Pierwsza strona kreatora (**Welcome Page**) informuje użytkownika o funkcjach operacji. Przeczytaj ją dokładnie i kliknij przycisk **Next**, aby kontynuować.

Druga strona (strona **Disk Image Placement**) proponuje określenie miejsca istniejącego obrazu dysku zaszyfrowanego.



Użytkownik może podać pełną ścieżkę do pliku obrazu na dysku twardym lub użyć do tego celu standardowego przeglądania plików. Aby rozpocząć przeglądanie plików, kliknij przycisk **Browse**. Po określeniu parametrów pliku obrazu, kliknij przycisk **Next**, aby kontynuować.

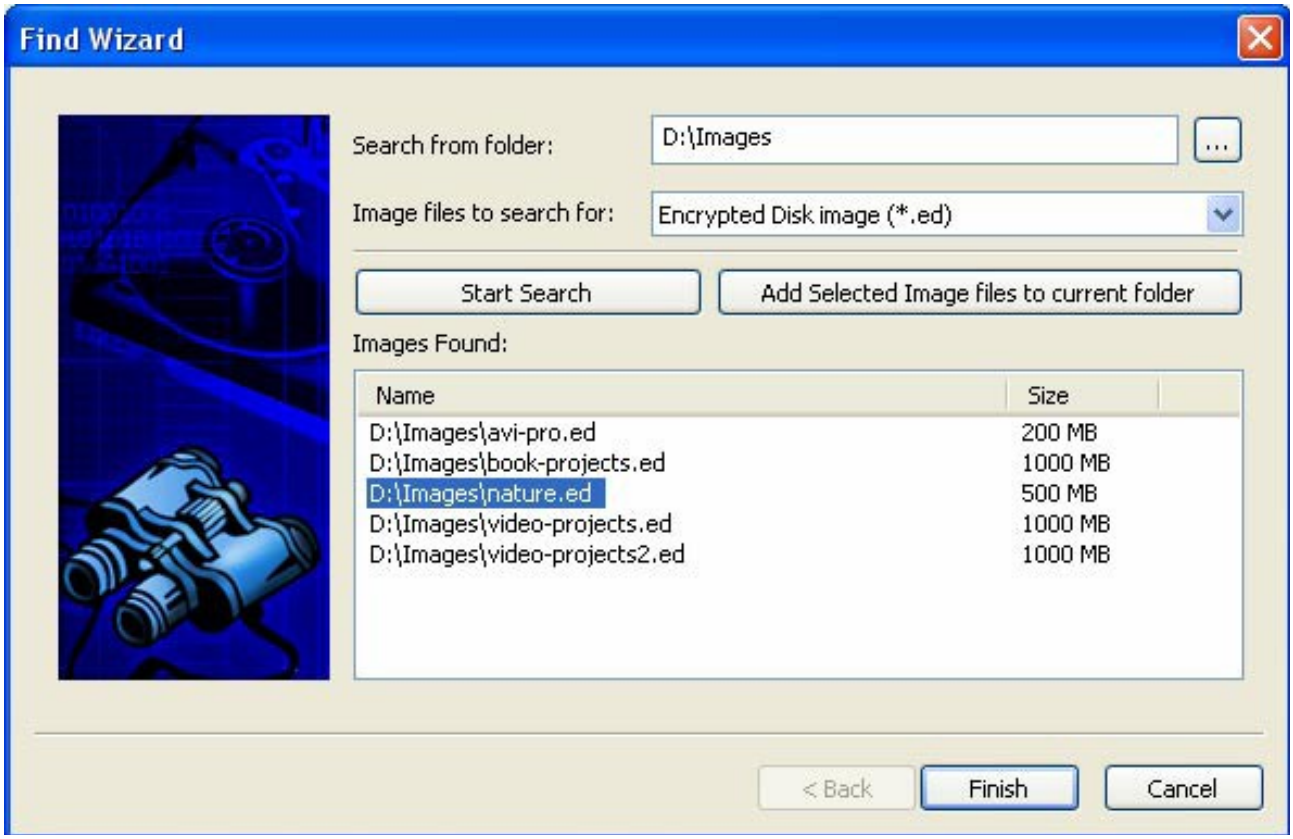
Trzecia strona (strona **Disk Image Encryption**) pozwala zmienić parametry szyfrowania dla wybranego dysku zaszyfrowanego. Użytkownik może wybrać inny algorytm szyfrowania lub zmienić jedynie metodę generowania klucza. Metoda generowania klucza określa czy klucz szyfrowania będzie generowany w oparciu o podane hasło czy w oparciu o dowolne zdarzenie systemowe (element **Key from file**). W ostatnim przypadku klucz będzie przechowywany w osobnym pliku na nośniku zewnętrznym.

Pola **Encryption algorithm** i **Key generator** opisane zostały w rozdziale Tworzenie dysków zaszyfrowanych. Jeśli zmieniony ma zostać tylko klucz szyfrowania lub hasło dla wybranego obrazu (bez zmiany algorytmu szyfrowania), należy wybrać odpowiednią opcję w górnej części strony – **Change only the encryption key used for this image**.
Kliknij przycisk **Next**, aby rozpocząć operację ponownego szyfrowania.

Strona kreatora **The completing** informuje użytkownika o pomyślnym utworzeniu nowego dysku zaszyfrowanego. Zmiany zostaną wprowadzone zaraz po zakończeniu pracy kreatora.

Wyszukiwanie dysków zaszyfrowanych

Kreator **Find Wizard** służy do wyszukiwania obrazów dysków zaszyfrowanych na lokalnych dyskach twardych. Znalezione obrazy zostaną selektywnie dołączone do bazy danych menadżera **Encrypted Disk Manager**.



Używaj kreatora **Find Wizard** w następujący sposób:

1. Uruchom kreatora **Find Wizard** (kliknij odpowiedni przycisk w pasku **Utilities bar**).

2. Wybierz w polu o nazwie **Search from folder** folder lub dysk, który ma zostać przeskanowany. Kreator **Find Wizard** przeskanuje ten folder i jego podfoldery.

3. Kliknij przycisk **Start search,** aby rozpocząć wyszukiwanie obrazów.

4. Program wyświetli znalezione obrazy w liście o nazwie **Images found**.

5. Można przerwać skanowanie przed zakończeniem procesu za pomocą przycisku **Stop** ulokowanego w dolnej części okna.

6. Wybierz obrazy, które mają zostać załączone w bazie danych.

7. Kliknij następnie przycisk **Add selected images to current folder**.

Program umieści wybrane obrazy w bieżącym folderze bazy danych menadżera **Encrypted Disk Manager**. Duplikaty zostaną zignorowane.

Dodawanie dysków zaszyfrowanych

W niektórych przypadkach konieczne jest dodanie obrazów dysku zaszyfrowanego utworzonego na innym komputerze lub obrazów, których lokalizacja została zmieniona. Może się to wydarzyć na przykład, kiedy plik obrazu został przeniesiony lub ulokowany na nośniku wymiennym.

Aby dodać taki obraz, uruchom menadżera **Encrypted Disk Manager**, a następnie wykonaj jedną

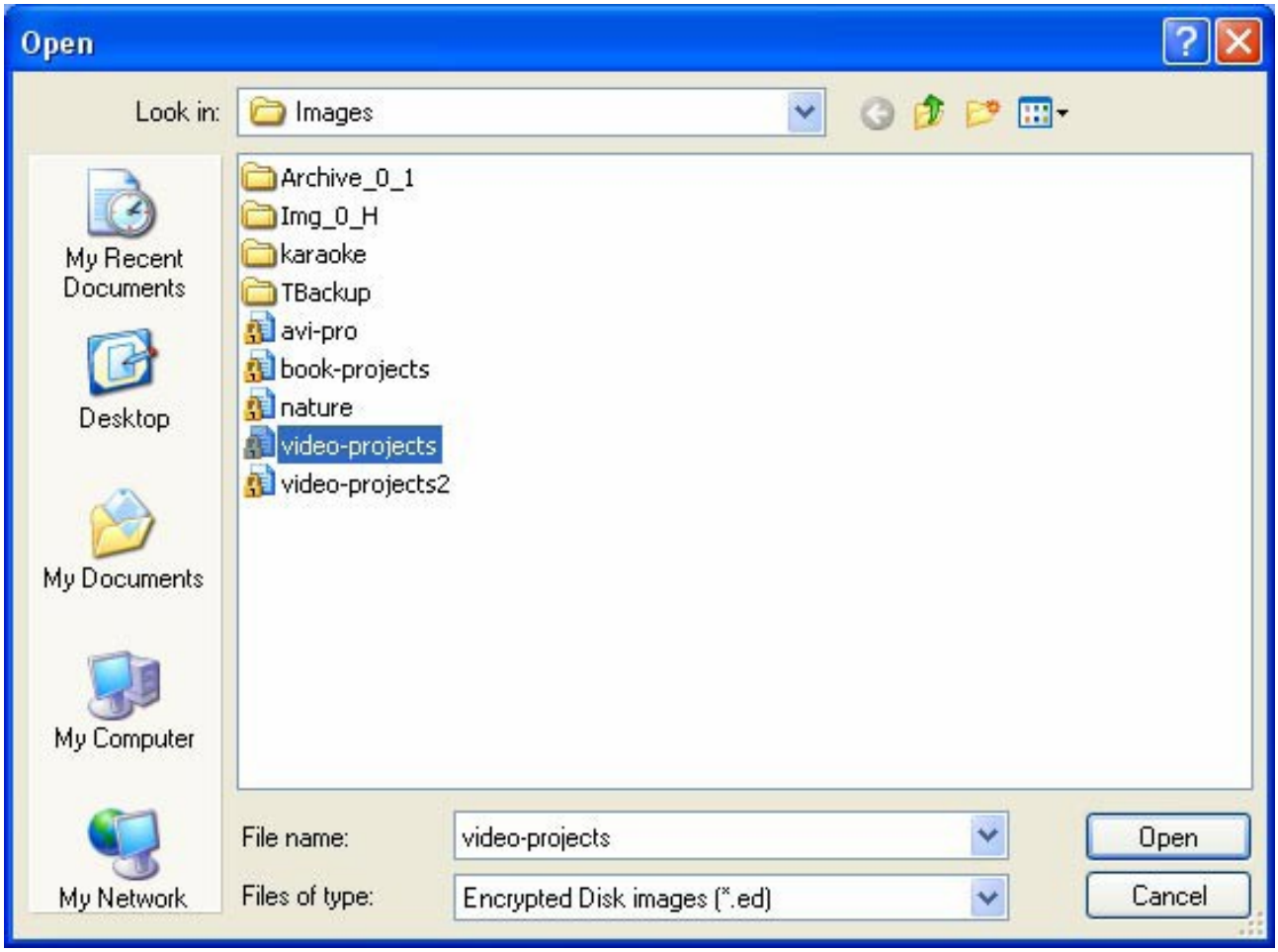
z następujących czynności:

• Wybierz element w main menu: **File > Add image**.

• Kliknij przycisk **Add image** w pasku tool bar.

• Wybierz element **Add image** w menu kontekstowym dowolnego folderu znajdującego się w bazie danych.

Po wykonaniu tych akcji pojawi się standardowe okno dialogowe **Open file**.



Wybierz wymagany plik obrazu, aby był dostępny w programie.

Montowanie dysków zaszyfrowanych

Dysk zaszyfrowany powinien być zamontowany, aby był dostępny w systemie w formie litery dysku. Program pozwala na zamontowanie jednocześnie 23 zaszyfrowanych dysków. Są trzy sposoby na zamontowanie dysków zaszyfrowanych.

Montowanie za pomocą paska zadań Windows System Tray

Użytkownik powinien wykonać następujące czynności:

1. Kliknij prawym przyciskiem myszy na ikonę **Encrypted Disk** w pasku zadań.

2. Wybierz w menu element **Mount**.

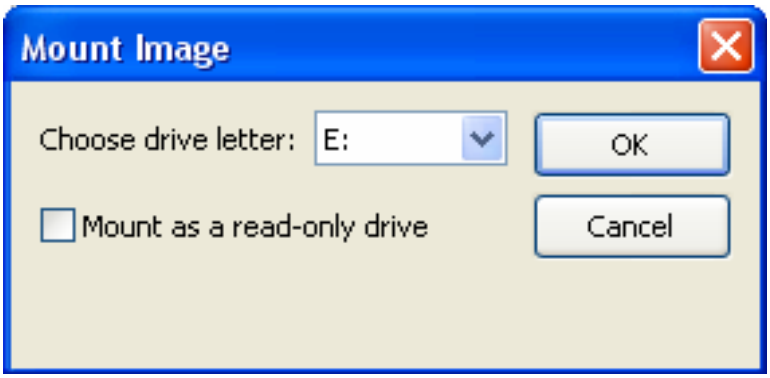
3. Wybierz plik obrazu dysku zaszyfrowanego, który zostanie zamontowany.

4. Wybierz literę dysku, jaka zostanie przypisana do dysku. (Do tego celu służy menu **Choose drive letter.** Zawiera ono pełną listę liter dysku dostępnych w systemie.)

5. Wybierz pole wyboru **Mount as a read-only-drive,** jeśli dysk ma być tylko do odczytu.

6. Kliknij przycisk **OK**.

Dwa ostatnie etapy wykonaj w specjalnym oknie dialogowym **Mount Image**.



Operacja zajmuje tylko kilka sekund. Dysk zaszyfrowany będzie reprezentowany w systemie jako zwyczajny dysk lokalny z przypisaną literą dysku.

Montowanie za pomocą eksploratora Windows

Użytkownik powinien wykonać następujące czynności:

1. Wybierz na dysku lokalnym plik obrazu dysku zaszyfrowanego.

2. Wybierz element **Encrypted Disk** w menu kontekstowym.

3. Wybierz element **Mount** w podmenu **Encrypted Disk.**

4. Wybierz literę dysku, jaka zostanie przypisana dla dysku. (Do tego celu służy menu **Choose drive letter.** Zawiera ono pełną listę liter dysku dostępnych w systemie.)

5. Wybierz pole wyboru **Mount as a read-only-drive,** jeśli dysk ma być tylko do odczytu.

6. Kliknij przycisk **OK**.

Dwa ostatnie etapy wykonaj w specjalnym oknie dialogowym **Mount Image**. Operacja zajmuje tylko kilka sekund. Dysk zaszyfrowany będzie reprezentowany w systemie jako zwyczajny dysk lokalny z przypisaną literą dysku.

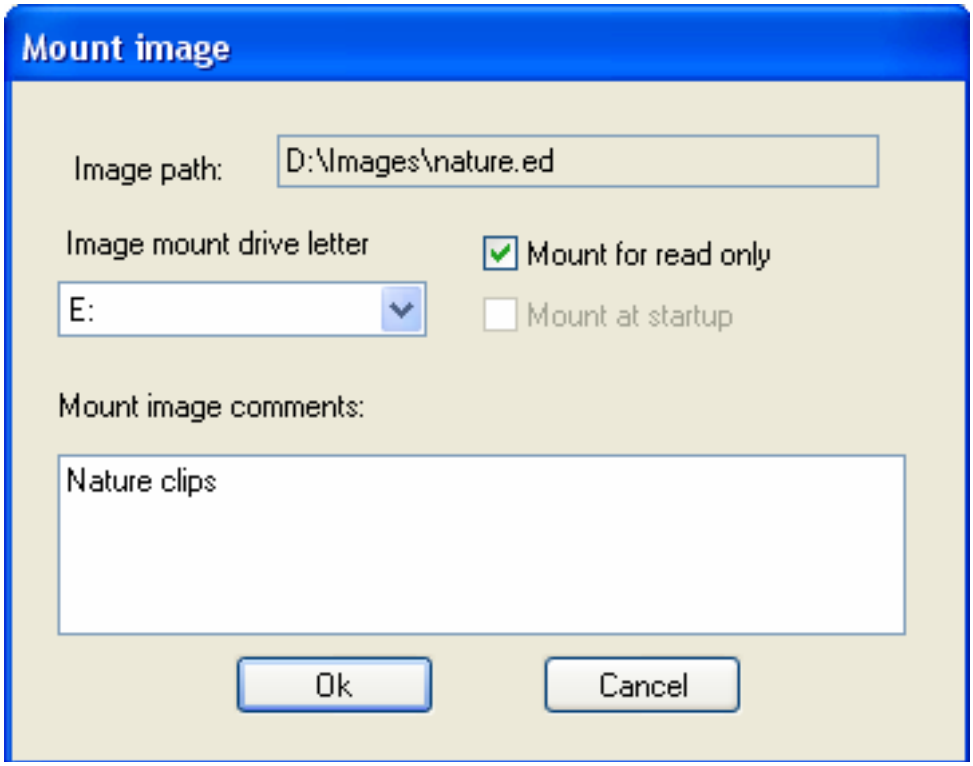
Montowanie za pomocą menadżera Encrypted Disk Manager

Menadżer **Encrypted Disk Manager** pozwala na rozpoczęcie tej operacji na kilka sposobów. Na początku użytkownik powinien wybrać obraz dysku zaszyfrowanego, a następnie:

• Wybierz w main menu element: **Actions > Mount**

• Kliknij przycisk **Mount** w pasku tool bar.

• Wybierz element **Mount** w menu kontekstowym dowolnego obrazu znajdującego się w bazie danych. Po wykonaniu tych czynności pojawi się specjalne okno dialogowe **Mount Image**. Różni się ono nieco od opisanego powyżej.



Okno to wskazuje pełną ścieżkę do wybranego pliku obrazu na dysku twardym w polu **Image path**. Menu **Image mount drive letter** zawiera pełną listę dostępnych w systemie liter dysku. Użytkownik powinien wybrać jedną do przypisania dla dysku zaszyfrowanego. Jeśli dysk ma być tylko do odczytu zaznacz pole wyboru **Mount for read only.** Użytkownik może dodać komentarz do montowanego obrazu w oddzielnym polu **Mount image comments**. Może on pomóc w odróżnieniu pewnych właściwości danych przechowywanych na tym dysku.

Odmontowanie dysków zaszyfrowanych

Użytkownik może odmontować dysk zaszyfrowany. Nie ma to wpływu na dane znajdujące się na tym dysku. Odmontowany dysk będzie jedynie niewidoczny w systemie i nie będzie możliwości pracy na nim. Później dysk może zostać ponownie zamontowany, aby była możliwość kontynuacji pracy.

Jeśli dysk zaszyfrowany używany jest przez jakiekolwiek inne oprogramowanie, wtedy próba odmontowania dysku doprowadzi do wyświetlenia informacji ostrzegawczej. Zalecane jest zamknięcie wszystkich otwartych plików i folderów dysku zaszyfrowanego i następnie ponowna próba odmontowania.

Opcja Forced Unmount może zostać użyta do natychmiastowego odmontowania zaszyfrowanych dysków, ale istnieje wysokie ryzyko utraty ważnych danych! Użyj tej opcji tylko w nagłych przypadkach, na przykład, kiedy prywatne dane mogą być zagrożone bezprawnym wkroczeniem z zewnątrz.

Istnieją trzy sposoby na odmontowanie dysku zaszyfrowanego.

Odmontowanie za pomocą paska zadań Windows System

Użytkownik powinien wykonać następujące czynności:

1. Kliknij prawym przyciskiem myszy na ikonę **Encrypted Disk** w pasku zadań.

2. Wybierz w menu element **Disks**.

3. Wybierz z listy literę dysku.

4. Wybierz w podmenu element **Unmount**.

Operacja zajmie kilka sekund. Dysk zaszyfrowany zniknie z systemu, ale wszystkie jego dane pozostaną niezmienione.

Istnieje możliwość odmontowania wszystkich dysków zaszyfrowanych. Aby wykonać tę operację, wykonaj następujące czynności:

1. Kliknij prawym przyciskiem myszy na ikonę **Encrypted Disk** w pasku zadań.

2. Wybierz w menu element **Disks**.

3. Wybierz w podmenu element **Unmount All**.

W ten sposób wszystkie dyski zaszyfrowane zamontowane w systemie zostaną odmontowane.

Odmontowanie za pomocą eksploratora Windows

Użytkownik powinien wykonać następujące czynności:

1. Wybierz dysk zaszyfrowany reprezentowany w systemie w formie litery dysku.

2. Wybierz w menu kontekstowym element **Encrypted Disk**.

3. Wybierz element **Unmount** w podmenu **Encrypted Disk**.

Litera dysku nie będzie przydzielona już dla dysku zaszyfrowanego i dostęp do niego nie będzie możliwy. Później użytkownik może ponownie zamontować dysk i kontynuować z nim pracę.

Odmontowanie za pomocą menadżera Encrypted Disk Manager

Menadżer **Encrypted Disk** pozwala na rozpoczęcie tej operacji na kilka sposobów. Początkowo użytkownik powinien wybrać obraz zamontowanego dysku zaszyfrowanego, a następnie:

• Wybierz w main menu element: **Actions > Unmount**

• Kliknij przycisk **Unmount** w pasku tool bar.

• Wybierz element **Unmount** w menu kontekstowym dowolnego obrazu znajdującego się w bazie danych.

Po wykonaniu tych czynności program informuje o pomyślnym odmontowaniu dysku.

Istnieje możliwość odmontowania wszystkich dysków zaszyfrowanych. Aby wykonać tę operację wybierz w main menu: **Actions > Unmount All**

Formatowanie dysków zaszyfrowanych

Jak każde inne dyski logiczne w systemie, zamontowane dyski zaszyfrowane powinny zostać sformatowane. Program obsługuje następujące typy systemów plików:

• FAT

• FAT32

• NTFS

Operacja formatowania wykonywana jest przez standardowe narzędzie systemu operacyjnego Windows. Aby sformatować dysk zaszyfrowany, użytkownik powinien wykonać następujące czynności:

1. Wybierz dysk w eksploratorze Windows (lub w innej dowolnej przeglądarce plików Windows, która obsługuje takie operacje).

2. Wybierz element **Format** w menu kontekstowym.

3. Określ parametry formatowania w oknie dialogowym **Format [:drive letter\]**. Dysk zaszyfrowany nie wymaga żadnych specjalnych parametrów dla tej operacji.

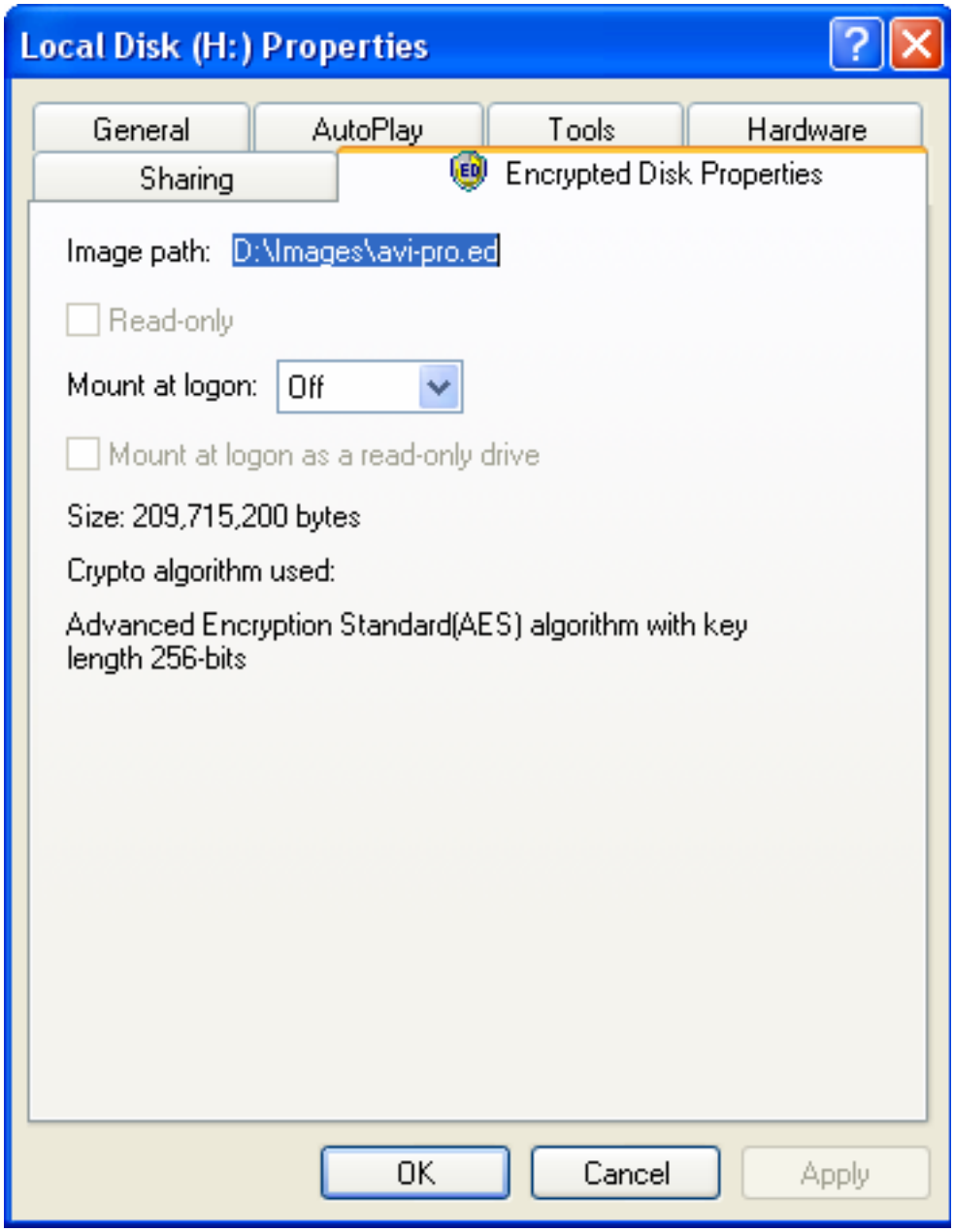
4. Kliknij przycisk **Start**.

Przeglądanie właściwości dysku zaszyfrowanego

Program pozwala na przeglądanie właściwości dysku zaszyfrowanego. Operacje tę można wykonać za pomocą eksploratora Windows lub menadżera **Encrypted Disk Manager**. Okna dialogowe właściwości różnią się w tych przypadkach.

Właściwości dysku zaszyfrowanego w eksploratorze Windows

Program dodaje specjalną kartę – **Encrypted Disk Properties** do standardowego okna dialogowego **Disk/ File properties**.



Górna linia okna dialogowego **Image path** wyświetla pełną ścieżkę do zamontowanych dysków oraz przypisaną dla pliku obrazu literę dysku obrazu (jeśli dysk nie jest zamontowany wyświetlone będzie – **Not mounted**).

Następne pole – **Read only** wskazuje czy dysk zaszyfrowany jest tylko do odczytu czy też nie.

Pole **Mount at logon** zawiera listę dostępnych liter dysku, które mogą być przypisane przy każdym zalogowaniu się użytkownika do systemu. Jeśli wybrany jest element **Off,** wtedy nie będzie montowany po zalogowaniu się użytkownika.

Istnieje możliwość montowania dysku zaszyfrowanego tylko do odczytu. Będzie to wykonywane automatycznie po każdym zalogowaniu użytkownika. Odpowiednie pole wyboru – **Mount at logon as read only drive** staje się dostępne po wybraniu litery dysku z listy wspomnianej powyżej.

Następne pole wyświetla rozmiar dysku zaszyfrowanego w bajtach.

Kolejne pole – **Crypto algorithm used** wyświetla algorytm jaki użyty został do zaszyfrowania dysku.

Właściwości dysku zaszyfrowanego w menadżerze ED Manager

Menadżer **Encrypted Disk Manager** zapewnia większą funkcjonalność w oknie dialogowym **Properties,** niż eksplorator Windows. Aby wywołać okno dialogowe, użytkownik powinien początkowo wybrać obraz dysku zaszyfrowanego, a następnie:

• Wybierz w main menu element: **File > Image Properties**

• Wybierz element **Image Properties** w menu kontekstowym.

Okno dialogowe posiada trzy party. Pierwsza z nich to **General,** przeznaczona do wyświetlenia standardowych informacji o pliku obrazu:

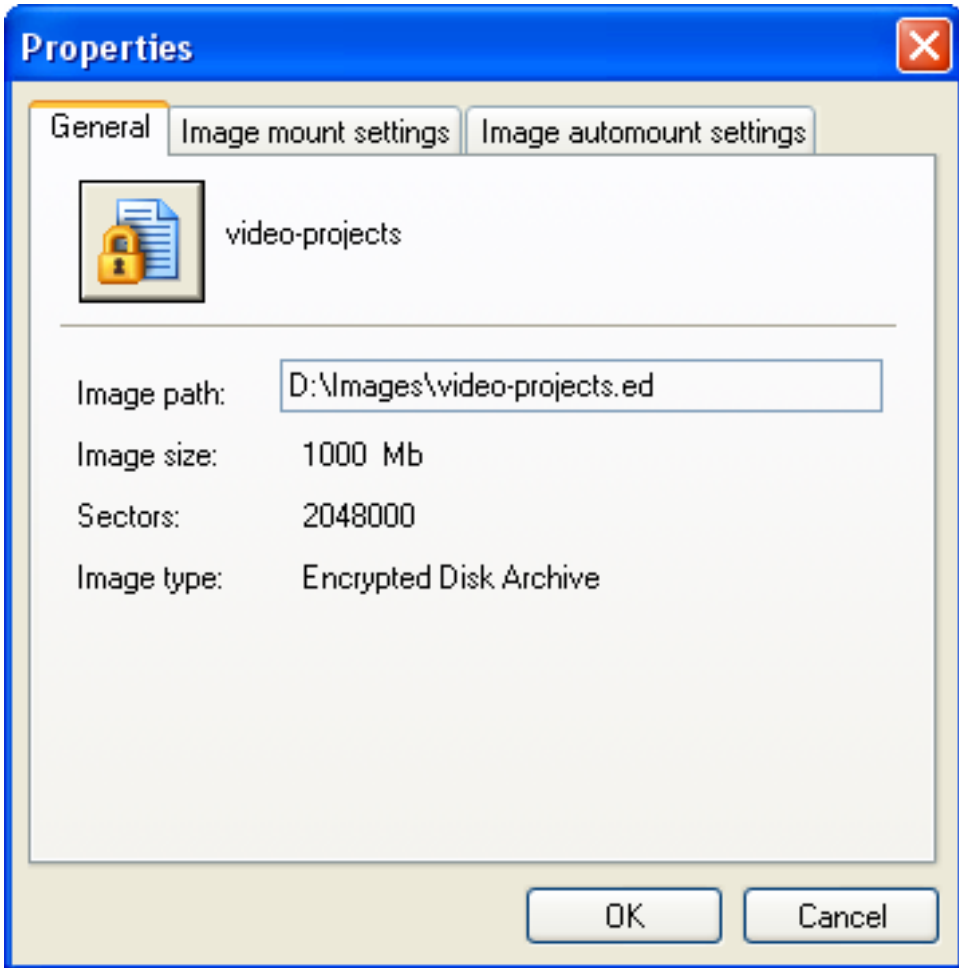
• Nazwa pliku obrazu;

• Pełna ścieżka do obrazu na dysku lokalnym (pole **Image path**);

• Rozmiar obrazu;

• Ilość sektorów na dysku zaszyfrowanym (pole **Sectors**);

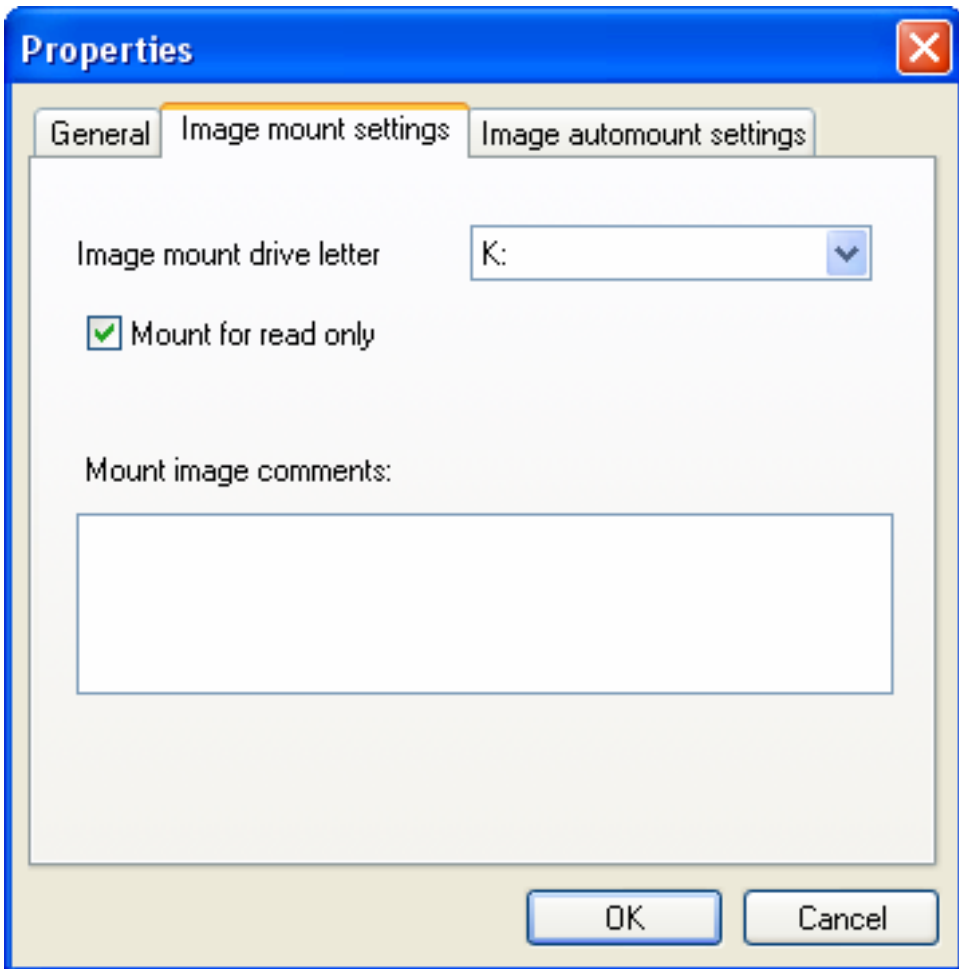
• Typ pliku (w tym przypadku **Encrypted Disk Archive**).



Druga karta **Image mount settings** służy do ustawienia parametrów montowania pliku obrazu. Za pomocą tej karty użytkownik może montować dyski zaszyfrowane jako dyski lokalne z dowolną dostępną literą dysku (pole **Image mount drive letter** zawiera pełną listę liter dysku, które dostępne są w systemie).

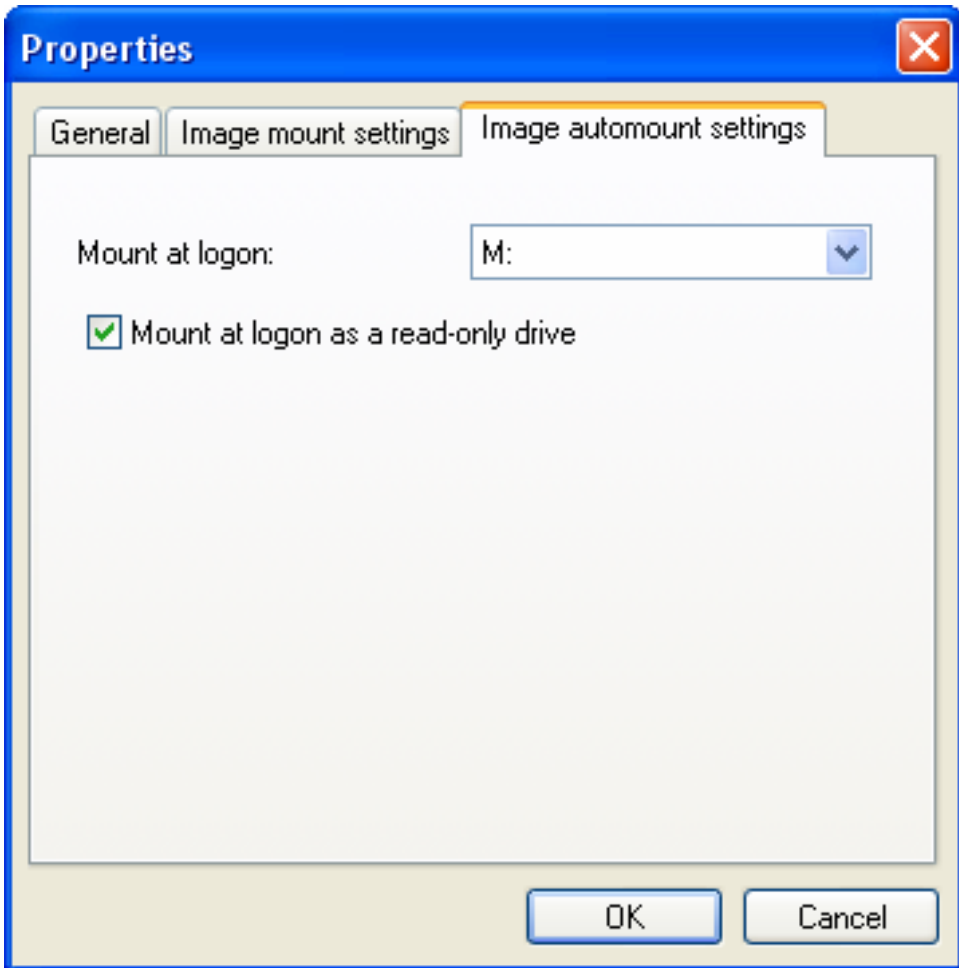
Pole wyboru **Mount for read only** pozwala na montowanie dysku zaszyfrowanego tylko do odczytu. Może być to przydatne, kiedy użytkownik nie zamierza zmieniać zawartości dysku.

Pole tekstowe **Mount image comments** pozwala na dodanie notatek dotyczących używania dysku lub danych jakie zawiera.



Trzecia karta – **Image automount settings** pozwala na ustawienie parametrów montowania, które zostaną zastosowane po zalogowaniu się użytkownika do systemu.

Menu **Mount at logon** zapewni listę dostępnych liter dysku. Użytkownik może wybrać jedną z nich, aby automatycznie została przypisana do dysku zaszyfrowanego. Jeśli dysk montowany jest tylko do odczytu wtedy należy użyć odpowiedniego pola wyboru **Mount at logon as a read-only drive**.



Wszystkie zmiany wprowadzone w oknie dialogowym **Properties** zostaną wprowadzone po kliknięciu w dole okna przycisku **OK**.

Udostępnianie dysków zaszyfrowanych

Dysk zaszyfrowany może zostać udostępniony jak każdy inny dysk logiczny. Pozwala to użytkownikowi na posiadanie serwera, na którym może przechowywać poufne informacje. Tylko użytkownicy grupy roboczej, w której udostępniony jest dysk zaszyfrowany mają dostęp do jego zawartości. W takim przypadku, jeden z użytkowników grupy, (a mianowicie administrator, który udostępnił dysk zaszyfrowany) powinien posiadać klucz szyfrowania lub znać hasło, aby kontrolować do niego dostęp. Zapewnia to poufność wewnętrznych informacji (informacji grupy wewnętrznej). Nawet jeśli dysk twardy serwera zostanie skradziony, nikt nie będzie miał możliwości odczytania informacji z dysków zaszyfrowanych, jak może się to stać w przypadku zwyczajnych partycji.

Usuwanie dysków zaszyfrowanych

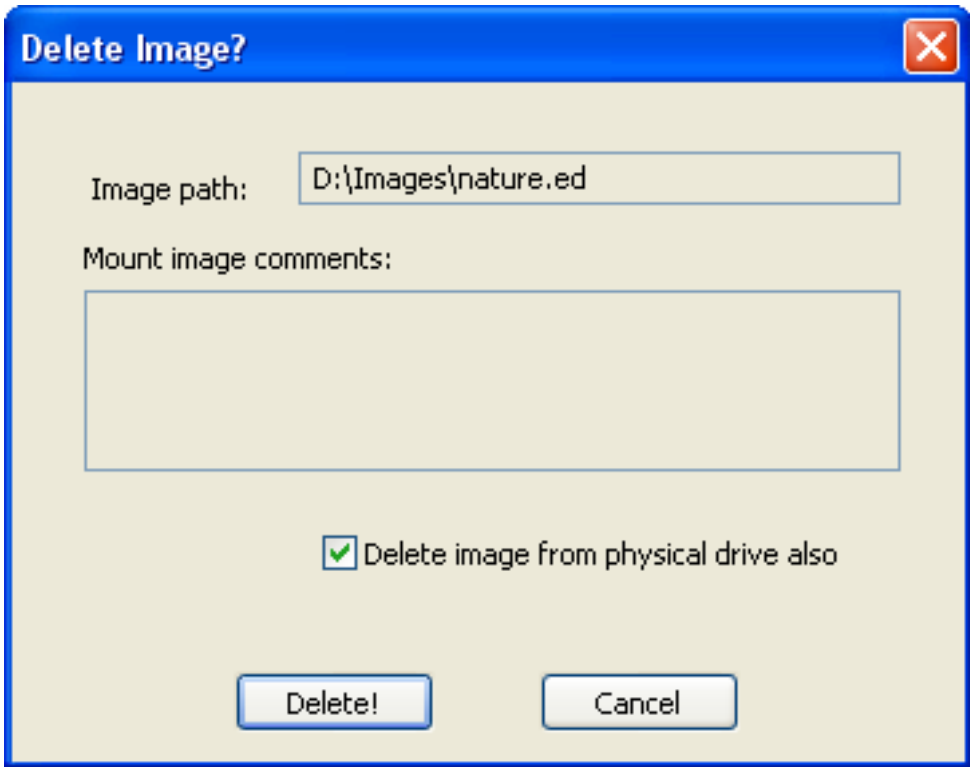
Użytkownik może usunąć istniejący dysk zaszyfrowany z bazy danych menadżera **Encrypted Disk Manager** lub fizycznie z lokalnego dysku twardego. Aby usunąć obraz, uruchom menadżera **Encrypted Disk Manager** i następnie wykonaj jedną z następujących czynności:

• Wybierz w main menu element: **File > Delete**

• Kliknij przycisk **Delete** w pasku tool bar.

• Wybierz element **Delete** w menu kontekstowym dowolnego obrazu dysku zaszyfrowanego.

Program poprosi użytkownika o potwierdzenie operacji w wyświetlonym oknie dialogowym **Delete Image**.



Użytkownik może zobaczyć pełną ścieżkę do pliku obrazu na dysku lokalnym (pole **Image path**) oraz przeczytać komentarze dotyczące pliku obrazu. Aby usunąć obraz fizycznie z dysku twardego, użytkownik powinien zaznaczyć pole wyboru **Delete image from physical drive also**. Jeśli to pole wyboru nie zostanie zaznaczone, obraz zostanie jedynie usunięty z bazy danych menadżera **Encrypted Disk Manager**.
Kliknij przycisk **Delete!,** aby potwierdzić wykonanie operacji.

Tylko odmontowane dyski zaszyfrowane mogą zostać usunięte fizycznie.