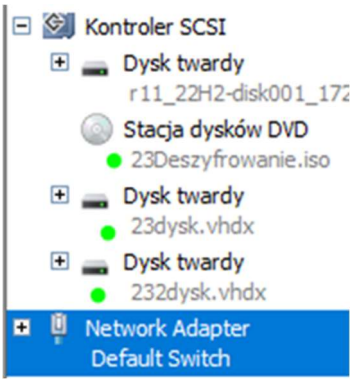
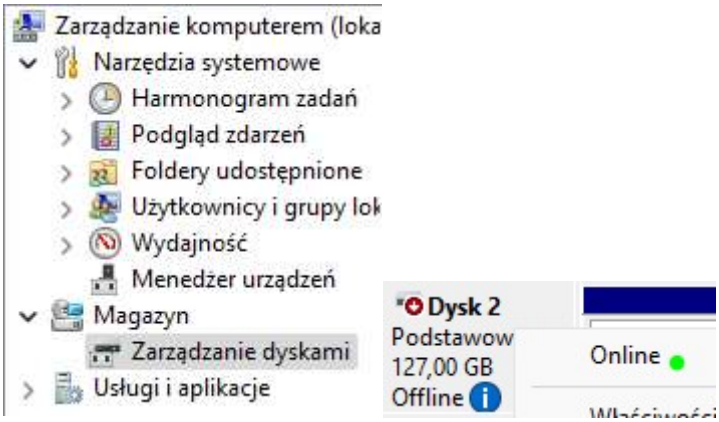
23.2 Deszyfrowanie danych, plików, dysków

Pobierz z materiałów i podłącz dodatkowo dysk 232dysk.vhdx oraz 23Deszyfrowanie.iso

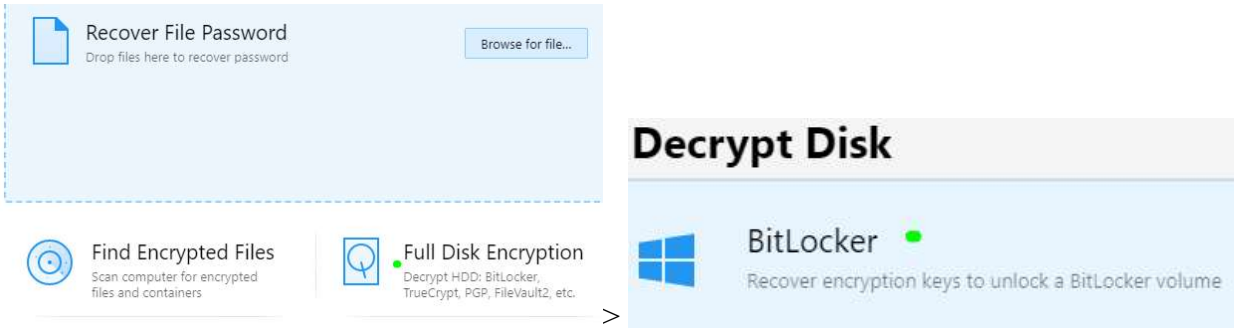


Upewnij się, że Network Adapter ustawiony jest jak na rysunku.



Włącz dysk ustawiony jest jak na rysunku.

Pobierz z CD/DVD lub Internetu i zainstaluj Passware



Jak odszyfrować funkcję BitLocker za pomocą zestawu Passware?

Odszyfrowywanie woluminów lub obrazów funkcji BitLocker jest trudne ze względu na różne opcje szyfrowania oferowane przez funkcję BitLocker, które wymagają różnych informacji do odszyfrowania.

Wyjaśnienie ochrony funkcji BitLocker i omówienie sposobu na odszyfrowanie danych, nawet na wyłączonych komputerach.

Opcje szyfrowania funkcją BitLocker

Zabezpieczenia, których można użyć do zaszyfrowania woluminu BitLocker, obejmują:

1. TPM (chip modułu zaufanej platformy)
2. TPM+PIN
3. Klucz startowy (na dysku USB)
4. TPM+PIN+klawisz uruchamiania
5. TPM + klawisz uruchamiania
6. Hasło
7. Klucz odzyskiwania (hasło numeryczne; na dysku USB)
8. Hasło odzyskiwania (na dysku USB)
9. Konto usług domenowych w usłudze Active Directory (AD DS)

Polecenie 1: Wyświetl listę zabezpieczeń danego woluminu funkcji BitLocker, wpisz następujące polecenie w wierszu polecenia (cmd): **manage-bde -protectors -get F:**

(gdzie F: jest nazwą zamontowanego woluminu zaszyfrowanego funkcją BitLocker)

Efekt: Lista zostanie wyświetlona w następujący sposób:

C:\WINDOWS\system32>manage-bde -protectors -get F:

BitLocker Drive Encryption: Configuration Tool version 10.0.19041

Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Volume F: [Label Unknown]

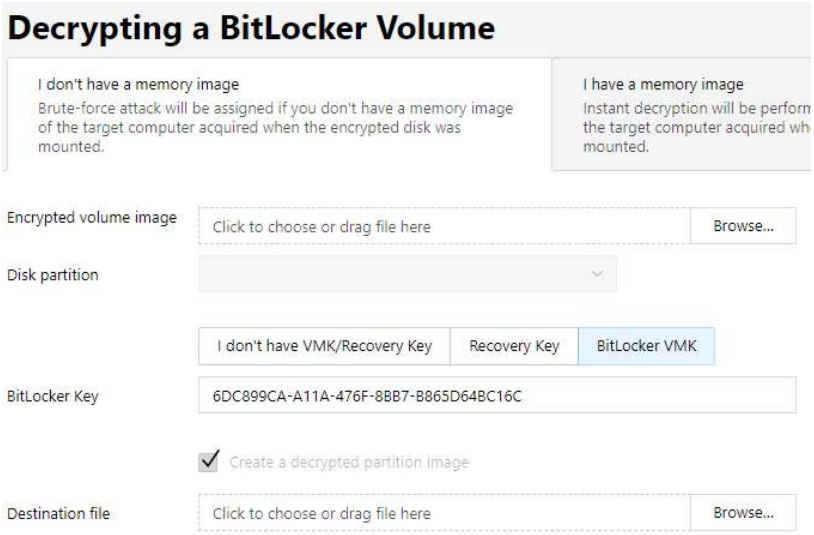
All Key Protectors

Password:

ID: {6DC899CA-A11A-476F-8BB7-B865D64BC16C}

Numerical Password:

ID: {CEE21E64-6D18-4C84-89BE-4D655961E931}



W wersji demo brak możliwości podłączenia dysku.

Szczegółowe informacje na temat każdego typu ochrany, zgodnie z dokumentacją Microsoft, znajdują się poniżej:

1. TPM. Funkcja BitLocker używa modułu TPM komputera do ochrony klucza szyfrowania. Jeśli określisz tę ochronę, użytkownicy będą mogli uzyskać dostęp do zaszyfrowanego dysku, o ile jest on podłączony do płyty systemowej, na której znajduje się moduł TPM, a integralność rozruchu systemu jest nienaruszona. Ogólnie zabezpieczenia oparte na module TPM można powiązać tylko z woluminem systemu operacyjnego.
2. TPM+PIN. Funkcja BitLocker wykorzystuje kombinację modułu TPM i dostarczonego przez użytkownika osobistego numeru identyfikacyjnego (PIN). Kod PIN składa się z czterech do dwudziestu cyfr lub, jeśli zezwalasz na ulepszone kody PIN, od czterech do dwudziestu liter, symboli, spacji lub cyfr.
3. Klucz uruchamiania. Funkcja BitLocker wykorzystuje dane wejściowe z urządzenia pamięci USB, które zawiera klucz zewnętrzny. Jest to plik binarny z rozszerzeniem .BEK.
4. TPM+PIN+Klucz uruchamiania. Funkcja BitLocker wykorzystuje kombinację modułu TPM, kodu PIN dostarczonego przez użytkownika i danych wejściowych z urządzenia pamięci USB zawierającego klucz zewnętrzny.
5. TPM + klucz uruchamiania. Funkcja BitLocker wykorzystuje kombinację modułu TPM i danych wejściowych z urządzenia pamięci USB, które zawiera klucz zewnętrzny.
6. Hasło. W celu uzyskania dostępu do woluminu używane jest hasło podane przez użytkownika.
7. Klucz odzyskiwania. Klucz odzyskiwania, zwany także hasłem numerycznym, jest przechowywany jako określony plik na urządzeniu pamięci USB. Jest to ciąg 48 cyfr podzielony myślnikami.

8. Konto usług domenowych w usłudze Active Directory. BitLocker używa uwierzytelniania domeny do odblokowywania woluminów danych. Woluminy systemu operacyjnego nie mogą używać tego typu ochrony klucza.

Każdy z tych zabezpieczeń szyfruje klucz główny woluminu BitLocker (VMK), aby wygenerować klucz szyfrowania pełnego woluminu (FVEK), który jest następnie używany do szyfrowania woluminu.

Utworzenie obrazu pamięci do natychmiastowego odszyfrowywania woluminów funkcji BitLocker

Polecenie 2: Utwórz obraz pamięci do natychmiastowego odszyfrowywania woluminów funkcji BitLocker, należy postępować zgodnie z poniższymi krokami:

1. Uruchom wiersz polecenia jako administrator.
2. Wpisz polecenie "manage-bde -protectors -get f:" i naciśnij Enter, gdzie "f:" oznacza literę dysku, który chcesz odszyfrować.
3. Skopiuj identyfikator zabezpieczeń dla woluminu BitLocker, który chcesz odszyfrować.
4. Wpisz polecenie "powershell" i naciśnij Enter, aby otworzyć konsolę PowerShell.
5. Wpisz polecenie "Suspend-BitLocker -MountPoint f: -RebootCount 0 -KeyProtectorId "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX"" i naciśnij Enter, gdzie "f:" oznacza literę dysku, który chcesz odszyfrować, a "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX" to identyfikator zabezpieczeń, który skopiowałeś w kroku 3.
6. Wykonaj obraz pamięci za pomocą narzędzia, takiego jak DumpIt **lub/i** WinPmem.

   Wykonanie obrazu pamięci (zrzutu pamięci) jest przydatne w analizie cyfrowej i zabezpieczeń, aby uchwycić stan pamięci RAM w danym momencie. Narzędzia takie jak DumpIt i WinPmem są popularne do tego celu. Oto jak można użyć obu tych narzędzi do wykonania obrazu pamięci:

   1. DumpIt

   DumpIt to prosty, darmowy program do tworzenia zrzutów pamięci, który nie wymaga instalacji. Oto kroki, jak go używać:

   1. **Pobierz DumpIt**:
      - Odwiedź stronę i pobierz wersję narzędzia.
   2. **Uruchom DumpIt**:
      - Otwórz folder, w którym pobrałeś DumpIt. Znajdziesz tam plik o nazwie DumpIt.exe.

- Kliknij prawym przyciskiem myszy na plik DumpIt.exe i wybierz "Uruchom jako administrator".

3. **Zgódź się na warunki**:
   - Po uruchomieniu pojawi się okno z prośbą o zaakceptowanie warunków licencji. Kliknij "I Agree", aby kontynuować.
4. **Wykonaj zrzut pamięci**:
   - DumpIt rozpocznie proces tworzenia zrzutu pamięci. Po zakończeniu operacji znajdziesz plik zrzutu pamięci w tym samym folderze, gdzie uruchomiłeś DumpIt. Plik będzie miał rozszerzenie .raw.

2. WinPmem

WinPmem to bardziej zaawansowane narzędzie do przechwytywania pamięci w systemach Windows. Oferuje więcej opcji konfiguracji i wsparcia dla różnych formatów. Oto jak używać WinPmem:

1. **Pobierz WinPmem**:
   - Odwiedź stronę WinPmem na GitHubie i pobierz najnowszą wersję z sekcji "Releases".
2. **Rozpakuj WinPmem**:
   - Rozpakuj pobrany plik ZIP do wybranego folderu.
3. **Uruchom WinPmem**:
   - Otwórz wiersz polecenia (cmd) lub PowerShell jako administrator.
   - Przejdź do folderu, w którym rozpakowałeś WinPmem. Na przykład:

```
cd C:\ścieżka\do\folderu\WinPmem
```

4. **Wykonaj zrzut pamięci**:
   - Wykonaj następujące polecenie, aby utworzyć zrzut pamięci:

```
.\winpmem_x64.exe --format raw --output C:\ścieżka\do\pliku\dump.raw
```

   - --format raw oznacza, że plik zrzutu będzie zapisany w formacie RAW. Możesz także użyć innych formatów, takich jak --format aff dla plików AFF (Advanced Forensic Format).
5. **Sprawdź plik**:
   - Po zakończeniu procesu znajdziesz plik zrzutu pamięci w określonej lokalizacji (C:\ścieżka\do\pliku\dump.raw).

Uwagi:

- **Uprawnienia**: Aby poprawnie wykonać zrzut pamięci, musisz mieć uprawnienia administratora na komputerze.
- **Bezpieczeństwo**: Wykonując zrzut pamięci, upewnij się, że masz odpowiednie uprawnienia i zgody, zwłaszcza w kontekście analizy śledczej lub audytów bezpieczeństwa.

- **Przechowywanie**: Zrzut pamięci może zawierać wrażliwe informacje, więc przechowuj go w bezpiecznym miejscu i chroń przed nieautoryzowanym dostępem.

7. Wpisz polecenie "Resume-BitLocker -MountPoint f:" i naciśnij Enter, gdzie "f:" oznacza literę dysku, który chcesz odszyfrować.
8. Zrestartuj komputer.

Po wykonaniu tych kroków będziesz miał obraz pamięci do natychmiastowego odszyfrowywania woluminów funkcji BitLocker. Pamiętaj jednak, że ten proces może naruszyć integralność danych na dysku, dlatego przed rozpoczęciem go zawsze należy wykonać kopię zapasową wszystkich ważnych plików.

Pomoc: Aby wznowić ochronę BitLockera na dysku F:, gdy napotykasz błąd, który sugeruje, że dysk jest zablokowany i musisz go odblokować przed wznowieniem ochrony, aby rozwiązać ten problem:

1. Odblokowanie Dysku

Zanim wznowisz ochronę BitLockera, upewnij się, że dysk jest odblokowany. Możesz to zrobić za pomocą PowerShell lub Panelu sterowania.

Za pomocą PowerShell

1. **Sprawdź Status Dysku**: Sprawdź, czy dysk jest odblokowany:

```
Get-BitLockerVolume -MountPoint f:
```

2. **Odblokuj Dysk**: Jeśli dysk jest zablokowany, użyj poniższego polecenia, aby go odblokować (zastąp YourPassword hasłem lub użyj odpowiedniego klucza ochrony):

```
Unlock-BitLocker -MountPoint f: -Password (ConvertTo-SecureString -String "YourPassword" -AsPlainText -Force)
```

Jeśli używasz klucza odzyskiwania zamiast hasła, użyj:

```
Unlock-BitLocker -MountPoint f: -RecoveryPassword "YourRecoveryPassword"
```

Za pomocą Panelu Sterowania

1. Otwórz **Panel sterowania**.
2. Przejdź do **System i zabezpieczenia** > **BitLocker Drive Encryption**.
3. Znajdź dysk F: i kliknij **Odblokuj dysk**.
4. Wprowadź hasło lub klucz odzyskiwania, aby odblokować dysk.

2. Wznowienie Ochrony

Po odblokowaniu dysku możesz wznowić ochronę BitLockera:

Za pomocą PowerShell

Resume-BitLocker -MountPoint f:

Za pomocą Panelu Sterowania

1. W Panelu sterowania przejdź do **System i zabezpieczenia** > **BitLocker Drive Encryption**.
2. Znajdź dysk F: i kliknij **Wznów ochronę**.

3. Sprawdzenie Statusu

Po wznowieniu ochrony upewnij się, że wszystko działa poprawnie:

Get-BitLockerVolume -MountPoint f:

4. Dodatkowe Rozwiązywanie Problemów

Jeśli nadal napotykasz problemy:

- **Sprawdź stan BitLockera**: Użyj manage-bde -status f: w wierszu poleceń, aby uzyskać więcej informacji o stanie dysku.
- **Sprawdź dzienniki systemowe**: Sprawdź dzienniki zdarzeń systemowych, aby uzyskać więcej informacji na temat błędów związanych z BitLockerem.

Polecenie 3: Odszyfrowywanie woluminów BitLocker z użyciem obrazów pamięci

Cel: Nauka procesu odszyfrowywania woluminów BitLocker przy użyciu obrazów pamięci i narzędzia Passware Kit.

Zadania:

1. **Teoria:**
    1. Wyjaśnij, czym jest VMK i FVEK w kontekście BitLocker.
    2. Opisz, jak system Windows używa TPM do montowania dysku systemowego przy domyślnych ustawieniach BitLocker.

Zapoznaj się z poniższym tekstem: Używanie obrazów pamięci do natychmiastowego odszyfrowywania woluminów funkcji BitLocker

Jeśli dany wolumin funkcji BitLocker jest zamontowany, VMK znajduje się w pamięci RAM.

Gdy system Windows wyświetla standardowy ekran logowania użytkownika systemu Windows, oznacza to, że wolumin systemowy funkcji BitLocker jest zamontowany, a VMK znajduje się w pamięci. Po utworzeniu obrazu pamięci na żywo przy użyciu metody gorącego rozruchu *, można użyć zestawu Passware Kit do wyodrębnienia VMK i odszyfrowania woluminu.

Po włączeniu komputera skonfigurowanego z domyślnymi ustawieniami funkcji BitLocker system Windows odczytuje klucz szyfrowania z układu TPM, montuje dysk systemowy i kontynuuje proces uruchamiania. W tym przypadku VMK również znajduje się w pamięci.

Passware Kit wyodrębnia VMK (format base64) z obrazu pamięci (lub pliku hibernacji), konwertuje go na FVEK i odszyfrowuje wolumin BitLocker. Odzyskuje również klucz odzyskiwania i zabezpieczenia klucza startowego, jeśli są dostępne.

Passware Kit Forensic wyświetla zarówno zabezpieczenia klucza szyfrowania/odzyskiwania, jak i klucza startowego (pliku), a także tworzy odszyfrowaną kopię woluminu.

2. **Praktyka:**

    1. Przygotuj środowisko testowe z zaszyfrowanym woluminem BitLocker.
    2. Utwórz obraz pamięci na żywo przy użyciu metody gorącego rozruchu.

    Krok 1: Przygotowanie narzędzi

    a. **Pobierz i zainstaluj narzędzie do tworzenia obrazów pamięci**: Możesz użyć narzędzi takich jak FTK Imager, **DumpIt**, czy Belkasoft Live RAM Capturer.

    b. **Przygotuj nośnik**: Upewnij się, że masz o odpowiedniej pojemności.

    Krok 2: Uruchomienie narzędzia

    a. **Upewnij się, że nośnik jest podłącz do komputera**: Upewnij się, że komputer jest włączony i działa.

    b. **Uruchom narzędzie do tworzenia obrazów pamięci**: Wybierz odpowiednie narzędzie i uruchom je z poziomu nośnika.

    Krok 3: Tworzenie obrazu pamięci

    a. **Wybierz opcję tworzenia obrazu pamięci**: W narzędziu wybierz opcję, która pozwala na utworzenie obrazu pamięci na żywo.

    b. **Wybierz lokalizację zapisu**: Wskaż miejsce, gdzie chcesz zapisać obraz pamięci (np. na nośniku).

c. **Rozpocznij proces tworzenia obrazu**: Kliknij przycisk, aby rozpocząć proces tworzenia obrazu pamięci. Może to potrwać kilka minut w zależności od wielkości pamięci RAM.

Krok 4: Zakończenie procesu

a. **Zapisz obraz pamięci**: Po zakończeniu procesu, upewnij się, że obraz pamięci został poprawnie zapisany na wybranym nośniku.

b. **Bezpiecznie odłącz nośnik**: Odłącz nośnik od komputera.

Krok 5: Analiza obrazu pamięci

a. **Użyj narzędzia Passware Kit**: Uruchom Passware Kit i załaduj utworzony obraz pamięci.

Krok 1: Uruchomienie Passware Kit

1. **Zainstaluj Passware Kit**: Upewnij się, że masz zainstalowaną najnowszą wersję Passware Kit na swoim komputerze.
2. **Uruchom program**: Kliknij ikonę Passware Kit, aby uruchomić program.

Krok 2: Załadowanie obrazu pamięci

1. **Wybierz opcję "BitLocker"**: W głównym menu Passware Kit wybierz opcję "BitLocker".
2. **Wybierz "Odszyfruj BitLocker"**: Kliknij na opcję "Odszyfruj BitLocker", aby rozpocząć proces.
3. **Załaduj obraz pamięci**: Kliknij przycisk "Dodaj plik" lub "Załaduj obraz pamięci" i wskaż lokalizację, gdzie zapisany jest obraz pamięci (np. na mopśnik).

b. **Wyodrębnij VMK**: Użyj Passware Kit do wyodrębnienia VMK z obrazu pamięci.

1. **Analiza obrazu pamięci**: Passware Kit rozpocznie analizę załadowanego obrazu pamięci w poszukiwaniu VMK.
2. **Wyodrębnienie VMK**: Po zakończeniu analizy, Passware Kit wyświetli znaleziony VMK w formacie base64.

c. **Odszyfruj wolumin BitLocker**: Przeprowadź konwersję VMK na FVEK i odszyfruj wolumin BitLocker.

Krok 1: Konwersja VMK na FVEK

1. **Konwersja klucza**: Passware Kit automatycznie przeprowadzi konwersję VMK na FVEK.

2. **Odszyfrowanie woluminu**: Użyj FVEK do odszyfrowania woluminu BitLocker. Passware Kit przeprowadzi ten proces automatycznie.

Krok 2: Zapis odszyfrowanego woluminu

1. **Wybierz lokalizację zapisu**: Wskaż miejsce, gdzie chcesz zapisać odszyfrowany wolumin.
2. **Zapisz odszyfrowany wolumin**: Kliknij przycisk "Zapisz", aby zakończyć proces.

2. **Analiza:**
   a. Przeanalizuj, jakie informacje są wyświetlane przez Passware Kit po odszyfrowaniu woluminu.
   b. Zapisz, jakie zabezpieczenia klucza szyfrowania/odzyskiwania oraz klucza startowego są dostępne po odszyfrowaniu.
3. **Dyskusja:**
   a. Zapisz jakie są potencjalne zagrożenia związane z przechowywaniem VMK w pamięci RAM?
   b. Zapisz jakie środki bezpieczeństwa można zastosować, aby chronić VMK przed nieautoryzowanym dostępem?

Materiały dodatkowe:

- Dokumentacja Passware Kit. Zapoznaj się z dokumentacją Passware Kit, aby uzyskać szczegółowe informacje na temat wszystkich funkcji i opcji.
- Artykuły na temat BitLocker i TPM

Dowiedz się więcej: learn.microsoft.com, odzyskiwanie-danych-z-dysku.warszawa.pl, en.wikipedia.org,

Zanotuj PODSUMOWANIE

Podsumowując, jeśli obraz pamięci zawiera VMK, wolumin zostanie odszyfrowany, niezależnie od typu ochrony użytej do zaszyfrowania woluminu. Wyodrębniając ten VMK, można również odzyskać zabezpieczenia (klucz odzyskiwania i klucz startowy).

Jeśli jednak obraz pamięci nie zawiera VMK (wolumin nie został zamontowany podczas pozyskiwania pamięci na żywo, plik hibernacji został nadpisany itp.), możliwe jest tylko odszyfrowanie woluminu za pomocą funkcji Ochrona hasła, czyli odzyskanie oryginalne hasło (przy użyciu ataków brute-force lub słownikowych).

Proces odzyskiwania hasła jest czasochłonny i zależy od złożoności hasła, wszelkiej wiedzy na temat hasła oraz zasobów sprzętowych dostępnych do odzyskiwania hasła, takich jak procesory graficzne i dostępność przetwarzania rozproszonego. W rezultacie odzyskane oryginalne hasło może zostać użyte do zamontowania woluminu funkcji BitLocker.

W przypadku niektórych woluminów hasło może nie znajdować się wśród używanych zabezpieczeń, a wolumin może być chroniony innymi zabezpieczeniami (np. kluczem uruchamiania lub TPM + PIN). W takim przypadku nie jest możliwe odszyfrowanie woluminu bez obrazu pamięci uzyskanego podczas zamontowania woluminu lub pliku hibernacji, który zawiera VMK.

* Ważne jest, aby uzyskać prawidłowy obraz pamięci na żywo, aby zachować rezydujące klucze szyfrowania. Gorący rozruch można przeprowadzić przy użyciu programu dystrybucyjnego systemu Linux zgodnego z bezpiecznym rozruchem systemu Windows, takiego jak program Passware Bootable Memory Imager dostępny w programie Passware Kit Forensic.