Odszyfrowanie dysku

Passware Kit Business i Passware Kit Forensic deszyfrują dyski twarde zaszyfrowane za pomocą:

1. BitLocker
2. TrueCrypt
3. VeraCrypt
4. LUKS/LUKS 2
5. FileVault2/APFS
6. McAfee EPE
7. DriveCrypt
8. PGP WDE/Symantec
9. Dysk Apple DMG
10. Ochrona danych firmy Dell

Passware Kit skanuje plik obrazu pamięci fizycznej (pozyskany podczas montowania zaszyfrowanego dysku, nawet jeśli komputer docelowy był zablokowany), wyodrębnia wszystkie klucze szyfrowania i odszyfrowuje dany wolumin. Takie obrazy pamięci można uzyskać za pomocą narzędzi innych firm, takich jak Passware Bootable Memory Imager, Belkasoft Live RAM Capturer , ManTech Physical Memory Dump Utility , Magnet RAM Capture, Digital Collector , osxpmem lub win32dd.

Jeśli komputer docelowy z zaszyfrowanym woluminem jest wyłączony, klucze szyfrowania nie są przechowywane w jego pamięci, ale prawdopodobnie można je odzyskać z pliku hiberfil.sys, który jest tworzony automatycznie podczas hibernacji systemu.

UWAGA: Jeśli komputer docelowy jest wyłączony, a zaszyfrowany wolumin został odmontowany podczas ostatniej hibernacji ani obraz pamięci, ani plik hiberfil.sys nie będą zawierały kluczy szyfrowania. Dlatego natychmiastowe odszyfrowanie woluminu jest niemożliwe. W takim przypadku Passware Kit przypisuje ataki brute-force w celu odzyskania oryginalnego hasła do woluminu, co jest procesem czasochłonnym.

Polecenie 1: Odszyfruj dysk z obrazu pamięci (przetestuj wszystkie podane sposoby):

1. **Uzyskaj obraz pamięci lub/i pobierz plik hiberfil.sys z komputera docelowego.**

a) Uzyskaj obraz pamięci systemu z komputera, musisz użyć specjalnego narzędzia, takiego jak Microsoft Windows Debugging Tools lub Sysinternals Suite, które jest dostępne na stronie internetowej firmy Microsoft.

Krok 1: Pobierz i zainstaluj narzędzie Debugging Tools lub Sysinternals Suite na swoim komputerze.

winget install Microsoft.WinDbg

Windows SDK — tworzenie aplikacji systemu Windows | Microsoft Developer

Pobierz pliki symboli systemu bezpośrednio z serwera symboli Microsoftu.:

1. **Utwórz katalog na symbole**:
   - Utwórz katalog C:\Symbols na wirtuanym komputerze.
2. **Skonfiguruj Debugging Tools for Windows**:
   - Otwórz Debugging Tools for Windows. WinDbg
   - Wpisz następujące polecenie, aby ustawić ścieżkę do symboli:

   .sympath SRV*C:\Symbols*https://msdl.microsoft.com/download/symbols
3. **Pobierz symbole**:
   - Symbole zostaną automatycznie pobrane do katalogu C:\Symbols podczas analizy zrzutu pamięci.
4. **Analiza zrzutu pamięci**:
   - Teraz możesz użyć polecenia dumpchk:

dumpchk -y C:\Symbols C:\memory.dmp

Krok 2: Uruchom narzędzie z uprawnieniami administratora.

Krok 3: W przypadku narzędzia Debugging Tools, wpisz wiersz polecenia "dumpchk -y <symbol path> <memory dump file>" (bez cudzysłowów), gdzie <symbol path> to ścieżka do pliku symboli systemu, a <memory dump file> to ścieżka do pliku obrazu pamięci systemu, którego chcesz odczytać.

Krok 4: W przypadku narzędzia Sysinternals Suite, uruchom program "RAMMap" i wybierz "Save" z menu "File", aby zapisać obraz pamięci systemu do pliku.

Pamiętaj, że uzyskanie obrazu pamięci systemu może być skomplikowane i wymagać pewnej wiedzy technicznej.

b) Uzyskaj plik hiberfil.sys z komputera, musisz wykonać następujące kroki:

1. Kliknij Wyszukaj i wpisz "cmd" w polu wyszukiwania, wybierz opcję "Uruchom jako administrator".
2. W oknie wiersza poleceń wpisz polecenie "powercfg.exe /hibernate off" i naciśnij klawisz Enter. To wyłączy funkcję hibernacji i usunie plik hiberfil.sys z systemu.
3. Teraz możesz skopiować plik hiberfil.sys z komputera, wykonując następujące kroki:

a. Przejdź do katalogu "C:"

b. W menu "Widok" wybierz opcję "Opcje".

c. W oknie "Opcje folderów" przejdź do zakładki "Widok".

d. Wybierz opcję "Pokaż ukryte pliki, foldery i dyski" i kliknij przycisk "OK".

e. Teraz plik hiberfil.sys powinien być widoczny w katalogu "C:". Skopiuj ten plik w dowolne miejsce, które wybierzesz.

4. Aby włączyć ponownie funkcję hibernacji, wpisz w oknie wiersza poleceń polecenie "powercfg.exe /hibernate on" i naciśnij klawisz Enter.

Uwaga: Hiberfil.sys jest chronionym systemowym plikiem, więc nie należy go usuwać lub modyfikować, chyba że wiesz dokładnie, co robisz.

Jeśli nie widzisz pliku **hiberfil.sys**, możliwe, że hibernacja nie była w pełni wyłączona lub plik został usunięty. Możesz spróbować ponownie włączyć i wyłączyć hibernację:

1. **Włącz hibernację**:
   - W wierszu poleceń jako administrator wpisz:
   powercfg.exe /hibernate on
   - Naciśnij **Enter** i uruchom ponownie komputer.
2. **Wyłącz hibernację**:
   - W wierszu poleceń jako administrator wpisz:
   powercfg.exe /hibernate off
   - Naciśnij **Enter** i uruchom ponownie komputer.

Wygląda na to, że Twój system nie obsługuje funkcji hibernacji z powodu ograniczeń w firmware, sprawdź lub zrób:

3. **Aktualizacja BIOS/UEFI**:
   - Sprawdź, czy jest dostępna aktualizacja BIOS/UEFI dla Twojego komputera. Aktualizacja może dodać wsparcie dla hibernacji. Odwiedź stronę producenta Twojego komputera lub płyty głównej, aby pobrać najnowszą wersję.(nie rób to maszyna wirtualna)
4. **Sprawdzenie ustawień BIOS/UEFI**:
   - Wejdź do BIOS/UEFI podczas uruchamiania komputera (zazwyczaj przez naciśnięcie klawisza F2, Del lub Esc).
   - Sprawdź, czy są dostępne ustawienia związane z zarządzaniem energią lub hibernacją i upewnij się, że są włączone.
5. **Sprawdzenie zgodności sprzętu**:
   - Niektóre starsze komputery mogą nie obsługiwać hibernacji. Sprawdź dokumentację swojego sprzętu, aby upewnić się, że jest zgodny z tą funkcją.

6. **Sprawdzenie ustawień systemowych**:
    - Upewnij się, że w systemie Windows nie są włączone funkcje, które mogą kolidować z hibernacją, takie jak Hyper-V, Device Guard lub Credential Guard[1].

Jeśli po wykonaniu tych kroków nadal nie możesz włączyć hibernacji, możliwe, że Twój sprzęt po prostu nie obsługuje tej funkcji.

Polecenie 2: Utwórz zaszyfrowany obraz dysku.

Utworzenie Plik obrazu zaszyfrowanego woluminu VeraCrypt

Aby utworzyć zaszyfrowany wolumin VeraCrypt w postaci pliku obrazu, należy postępować zgodnie z poniższymi krokami:

1. Pobierz i zainstaluj VeraCrypt z oficjalnej strony internetowej: https://www.veracrypt.fr/en/Downloads.html
2. Uruchom VeraCrypt i kliknij przycisk "Create Volume".
3. W oknie "VeraCrypt Volume Creation Wizard" wybierz opcję "Create an encrypted file container".
4. Wybierz miejsce, w którym chcesz zapisać plik obrazu zaszyfrowanego woluminu i nadaj mu nazwę.
5. Wybierz algorytm szyfrowania i klucz szyfrowania. Możesz wybrać jeden z domyślnych algorytmów lub utworzyć niestandardowy algorytm.
6. Określ rozmiar woluminu. Możesz utworzyć wolumin o dowolnym rozmiarze, ale pamiętaj, że musisz mieć wystarczającą ilość miejsca na dysku, aby go przechować.
7. Utwórz hasło i wpisz je dwa razy, aby potwierdzić.
8. Określ plik klucza i wybierz opcję tworzenia pliku klucza lub pomijania tej opcji.
9. W przypadku tworzenia pliku klucza wybierz miejsce, w którym chcesz zapisać plik i nadaj mu nazwę.
10. Wpisz "Random Data" w pole "Format options" i kliknij przycisk "Format".
11. Zaczekaj, aż VeraCrypt utworzy plik obrazu zaszyfrowanego woluminu.
12. Kliknij przycisk "Exit", aby zamknąć VeraCrypt.

Teraz masz gotowy plik obrazu zaszyfrowanego woluminu, który możesz montować w VeraCrypt i korzystać z niego jak z zwykłego woluminu. Aby zamontować plik obrazu, wystarczy uruchomić VeraCrypt, wybrać opcję "Select File" i wybrać plik obrazu zaszyfrowanego woluminu. Następnie wpisz hasło i kliknij przycisk "Mount".

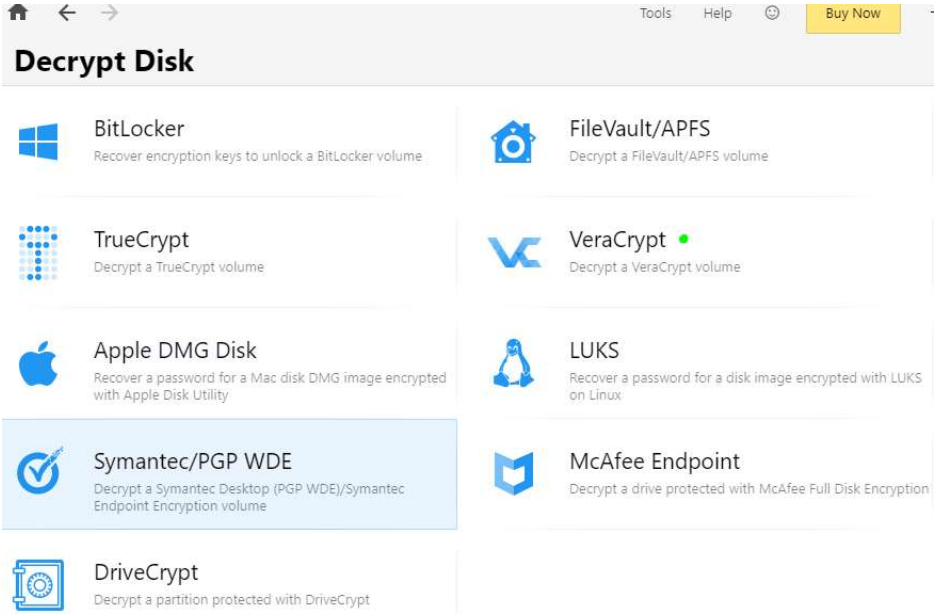
Polecenie 3: Uruchom Passware Kit, odzyskaj klucze szyfrowania i odszyfruj dysk twardy.

Poniżej znajdują się kroki, aby odszyfrować obraz dysku twardego.

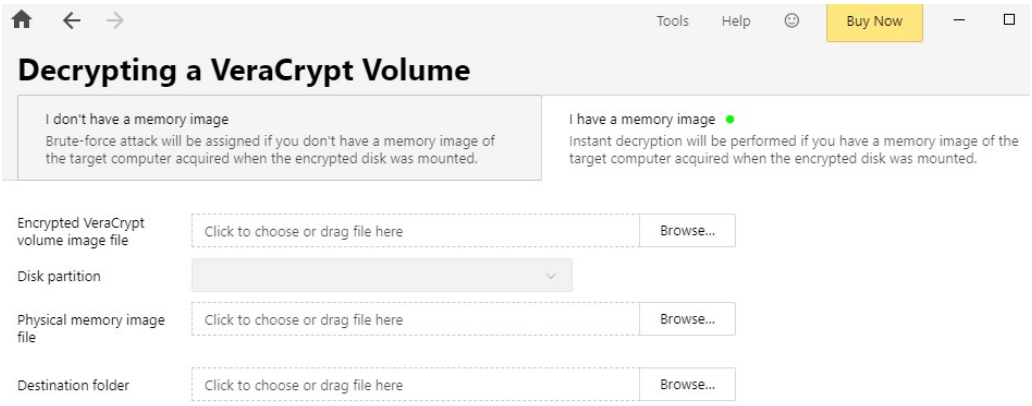
Odszyfrowywanie dysku twardego (kontener VeraCrypt)

Passware Kit może pracować z plikiem woluminu VeraCrypt (.HC, kontener zaszyfrowanego pliku) lub z jego obrazem. W przypadku odszyfrowywania BitLocker/FileVault2/PGP, Passware Kit działa z plikami obrazów zaszyfrowanych dysków. Obrazy woluminów dyskowych można tworzyć za pomocą narzędzi innych firm, takich jak X-Ways Forensics , OpenText EnCase Forensic, DD lub innych firm zewnętrznych .

1. Kliknij opcję Pełne szyfrowanie dysku na stronie startowej zestawu Passware Kit. Spowoduje to wyświetlenie ekranu pokazanego poniżej:

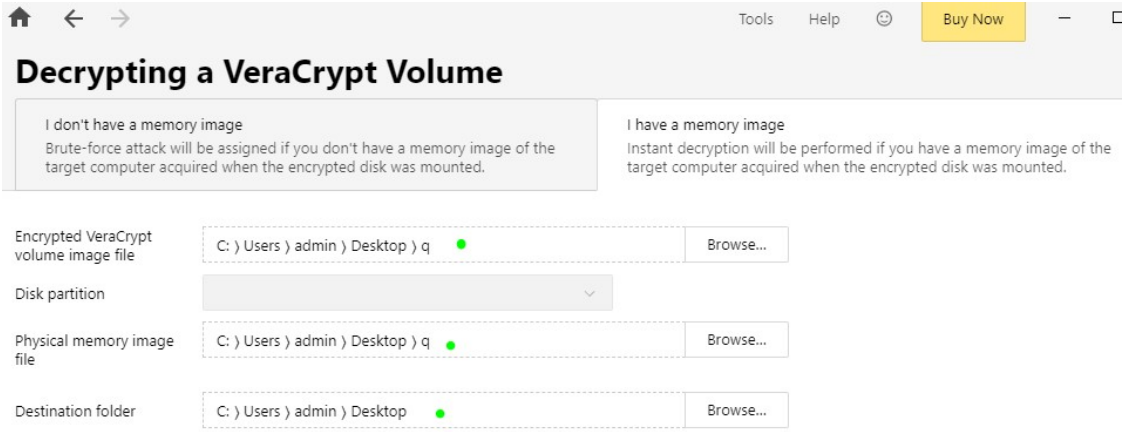


2. Kliknij odpowiedni typ szyfrowania, np. VeraCrypt. Spowoduje to wyświetlenie ekranu pokazanego poniżej:

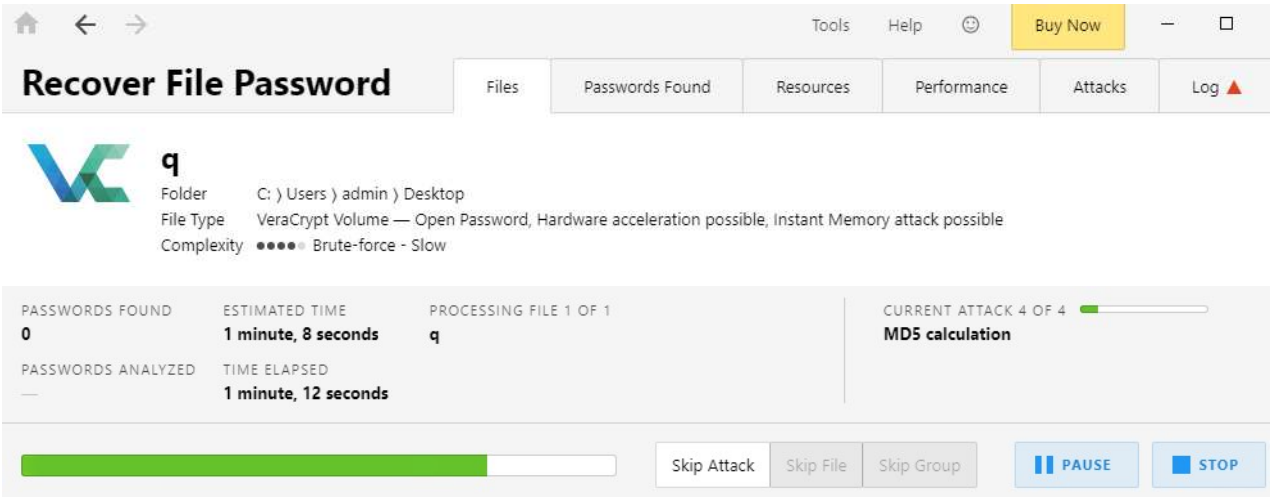


3. W polu Plik obrazu zaszyfrowanego woluminu VeraCrypt kliknij Przeglądaj…, ustaw Wszystkie pliki (*.*) z rozwijanego menu pola Nazwa pliku i zlokalizuj plik vc.hc.

Odszyfrowany obraz woluminu zostanie zapisany w lokalizacji pliku docelowego.



4. W polu Plik obrazu pamięci fizycznej kliknij Przeglądaj… i zlokalizuj plik. bin (lub plik hiberfil.sys z komputera, na którym zamontowano zaszyfrowany wolumin) Kliknij Odszyfruj:



UWAGA: Jeśli komputer docelowy jest wyłączony, a zaszyfrowany wolumin został odmontowany podczas ostatniej hibernacji ani obraz pamięci, ani plik hiberfil.sys nie będą zawierały kluczy szyfrowania. Dlatego natychmiastowe odszyfrowanie woluminu jest niemożliwe. W takim przypadku przełącz się na opcję „Nie mam obrazu pamięci", a Passware Kit przypisze ataki brute-force w celu odzyskania hasła do woluminu.

Passware Kit Forensic odzyskuje również hasła do kontenerów TrueCrypt i VeraCrypt oraz woluminów chronionych za pomocą plików kluczy. W ustawieniach odzyskiwania hasła (na karcie „Nie mam obrazu pamięci") Passware Kit pozwala użytkownikowi określić jeden lub więcej plików kluczy do sprawdzenia w połączeniu z hasłami. W rezultacie Passware Kit

wyświetla odzyskane hasło, które można wykorzystać do zamontowania woluminu przy użyciu określonych plików kluczy.

5. Passware Kit wyodrębnia klucz szyfrowania woluminu VeraCrypt i używa go do odszyfrowania kontenera. Oprogramowanie wyświetla również algorytm szyfrowania VeraCrypt używany do ochrony woluminu: