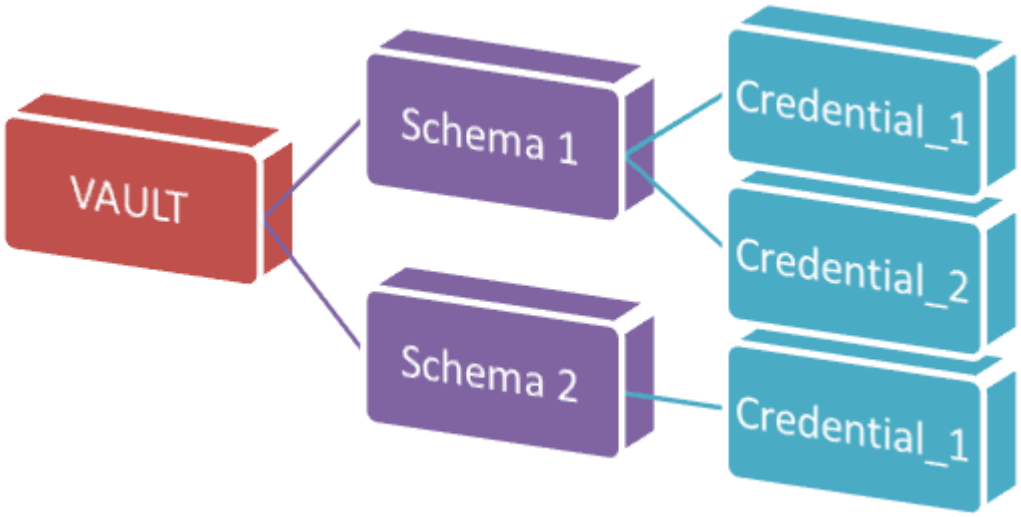
Windows Vault analyzer and decoder

Archived: 2026-04-05 20:22:37 UTC

Windows Password Recovery - Vault Explorer and Decoder

What is Windows Vault

Windows Vault is a protected storage for user or system secrets, passwords, network keys, web password and other personal information. Data stored in Windows Vault is structured and represents a set of records belonging to a certain Vault schema (see pic. below).



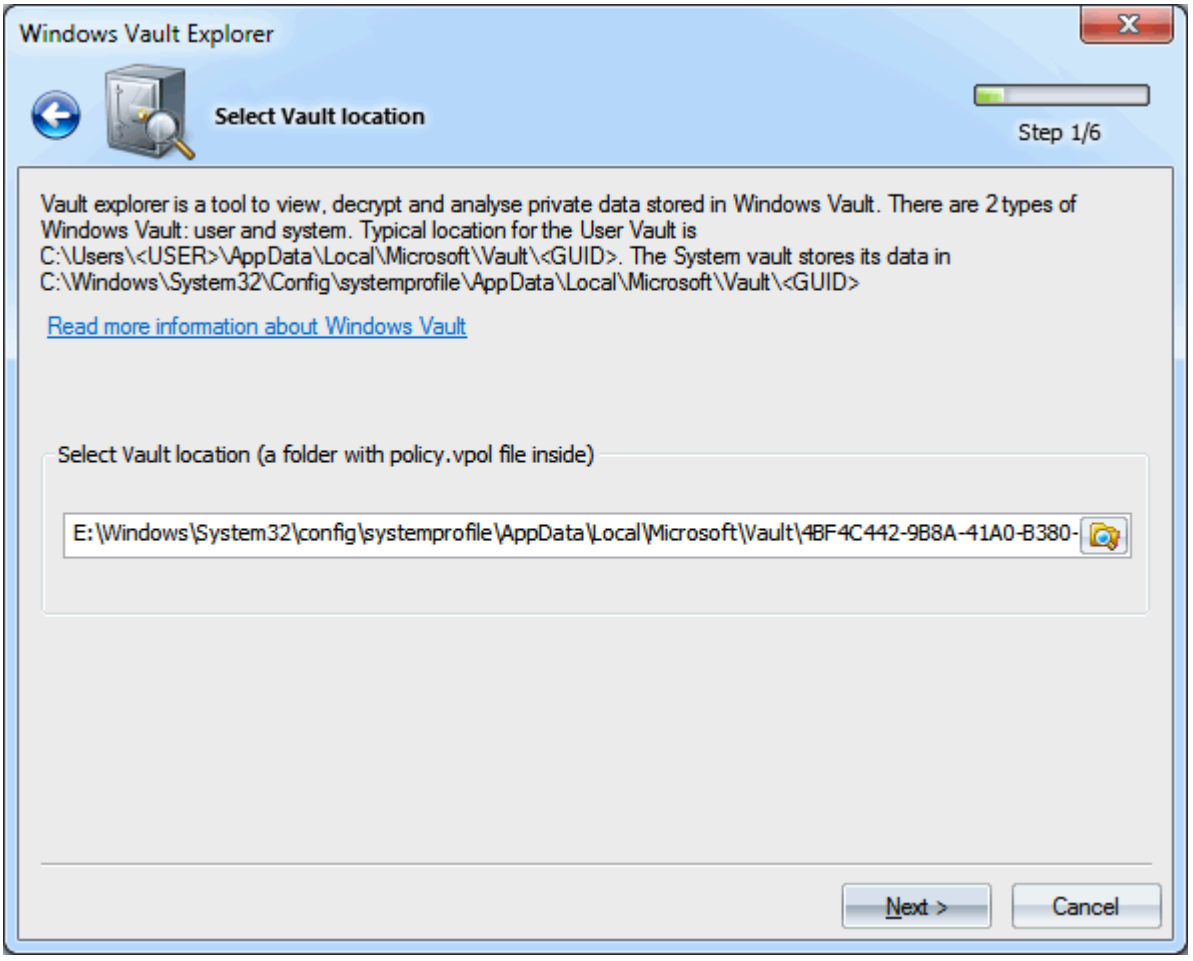
On the physical level, Vault is a disk-based folder with a set of the following files:

- ***Policy.vpol*** - set of encryption keys for Vault records (credentials). These keys can be protected using two basic methods: either using DPAPI or using a specific user password. The latter protection method is not used in Windows 8 and currently is not supported by the software.
- ***.vsch*** - Vault schema that contains data description, flags and other system information.
- ***.vcrd*** - Vault credential that stores the original encrypted data associated with a certain schema. The data normally consist of several fields. The description of the fields is stored in .vsch.

Windows Vault Explorer

Windows Vault Explorer is a utility for offline analyzing and decrypting Vault credentials. The decryption Wizard splits the entire process into the following steps:

Looking for Vault folder



There are currently two types of Vault storage: system and user. The user Vault storage can be located in the following folders:

```
%USER_APPDATA%\Microsoft\Vault\
%USER_LOCAL_APPDATA%\Microsoft\Vault\
```

For example,
C:\Users\John\AppData\Local\Microsoft\Vault\18289F5D-9783-43EC-A50D-52DA022B046E
C:\Users\Helen\AppData\Roaming\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28

The default location of the system Vault storage is:

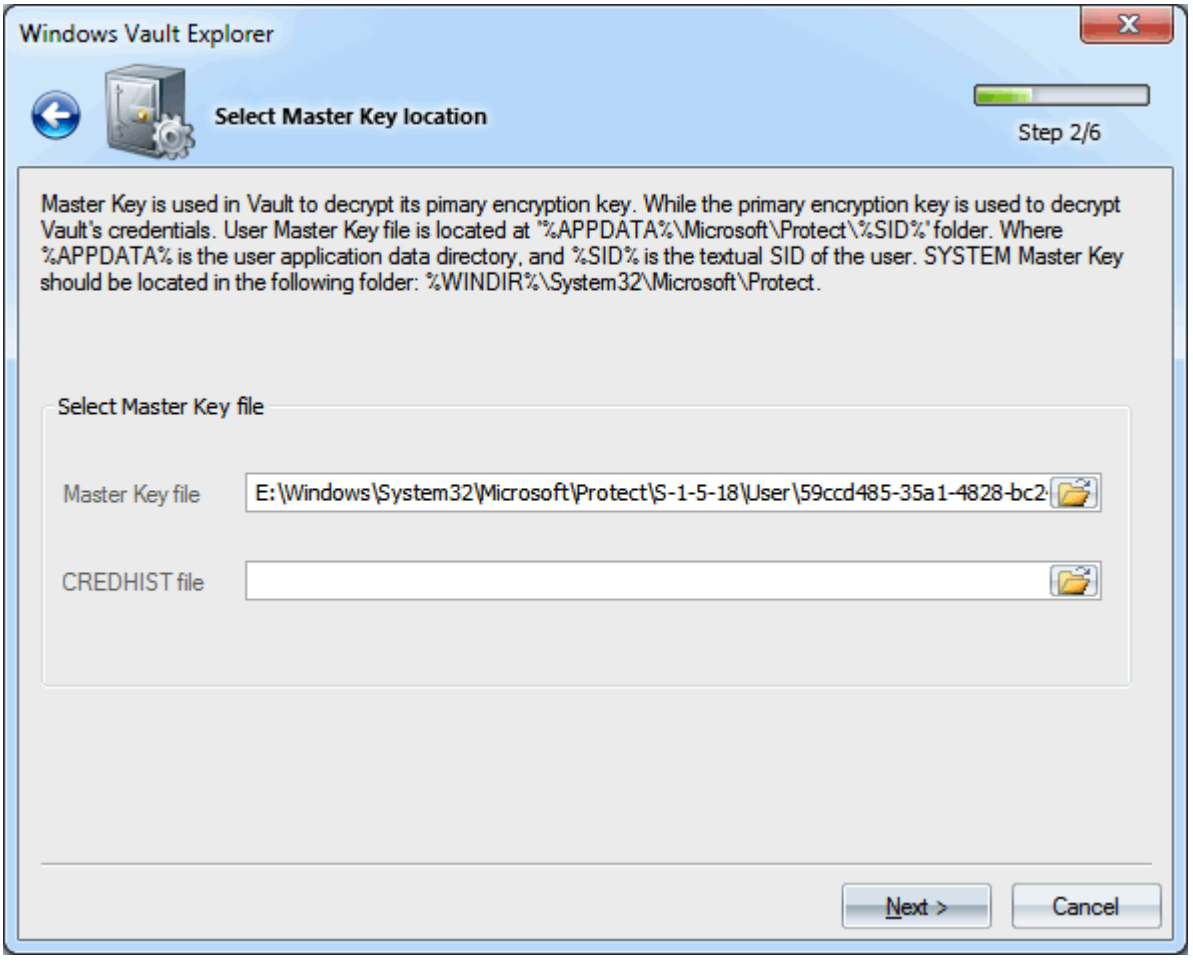
```
%SYSTEM_APPDATA%\Microsoft\Vault\
%SYSTEM_LOCAL_APPDATA%\Microsoft\Vault\
%PROGRAMDATA%\Microsoft\Vault\
```

For example,
C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28
C:\Windows\System32\config\systemprofile\AppData\Roaming\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28
C:\ProgramData\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204

Note that some of the specified folders have the system attribute set on, which makes these folders hidden.

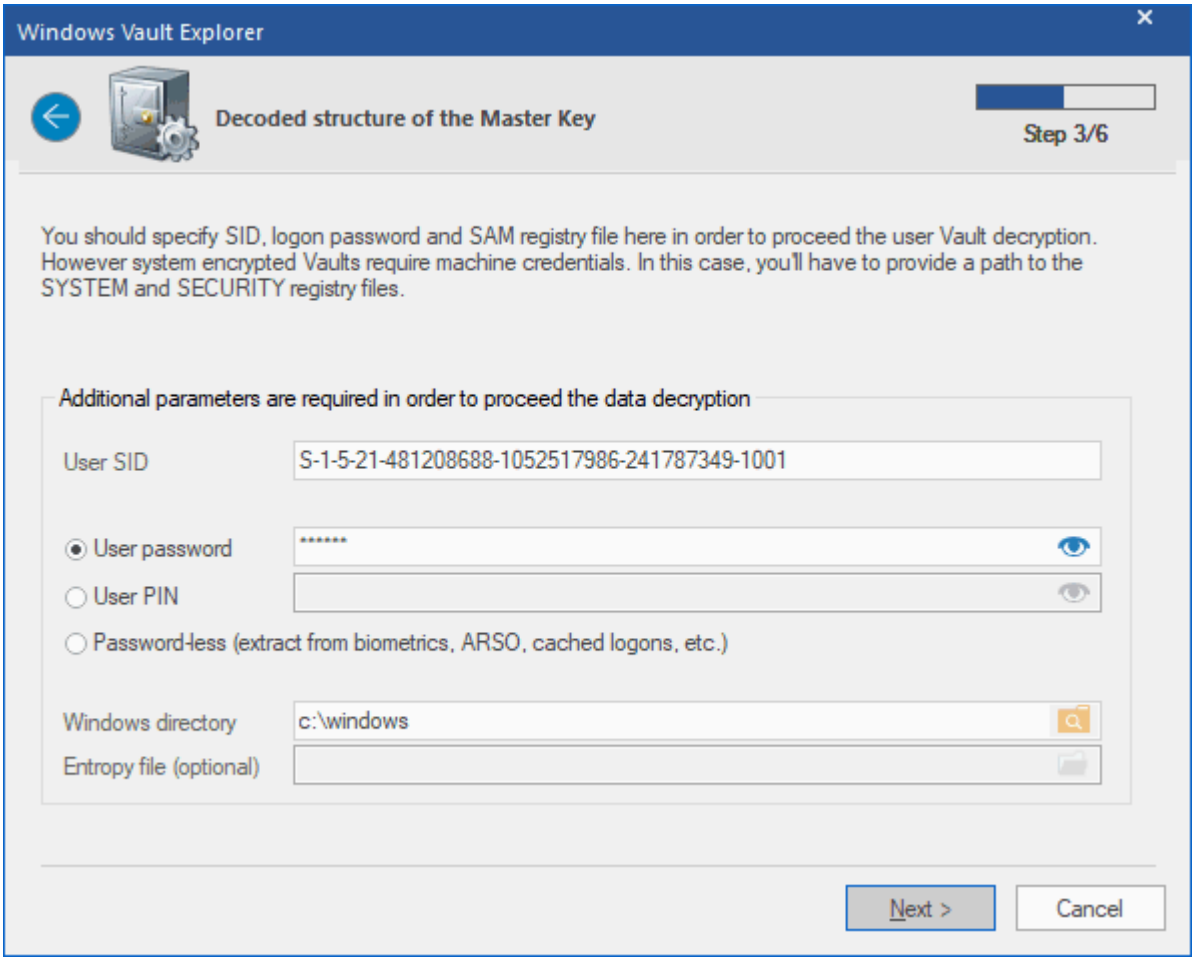
Windows has VaultCmd.exe utility for creating and managing your own Vault storages.

Selecting Master Key



Once a certain Vault folder is selected, you need to specify the path to the Master Key used in the protection of the Vault encryption keys. The user's Master Key always resides in the folder **%APPDATA%\Microsoft\Protect\%SID%**, and the system account's Master Keys are stored in **%SYSTEMDIR%\Microsoft\Protect**. It's worth mentioning that a typical user account contains several Master Keys, while a specific object could be decrypted using only one of them, the name of which is stored in the **Policy.vpol** file. When searching for the Master Key, the program can filter out unnecessary names.

Decrypting Master Key



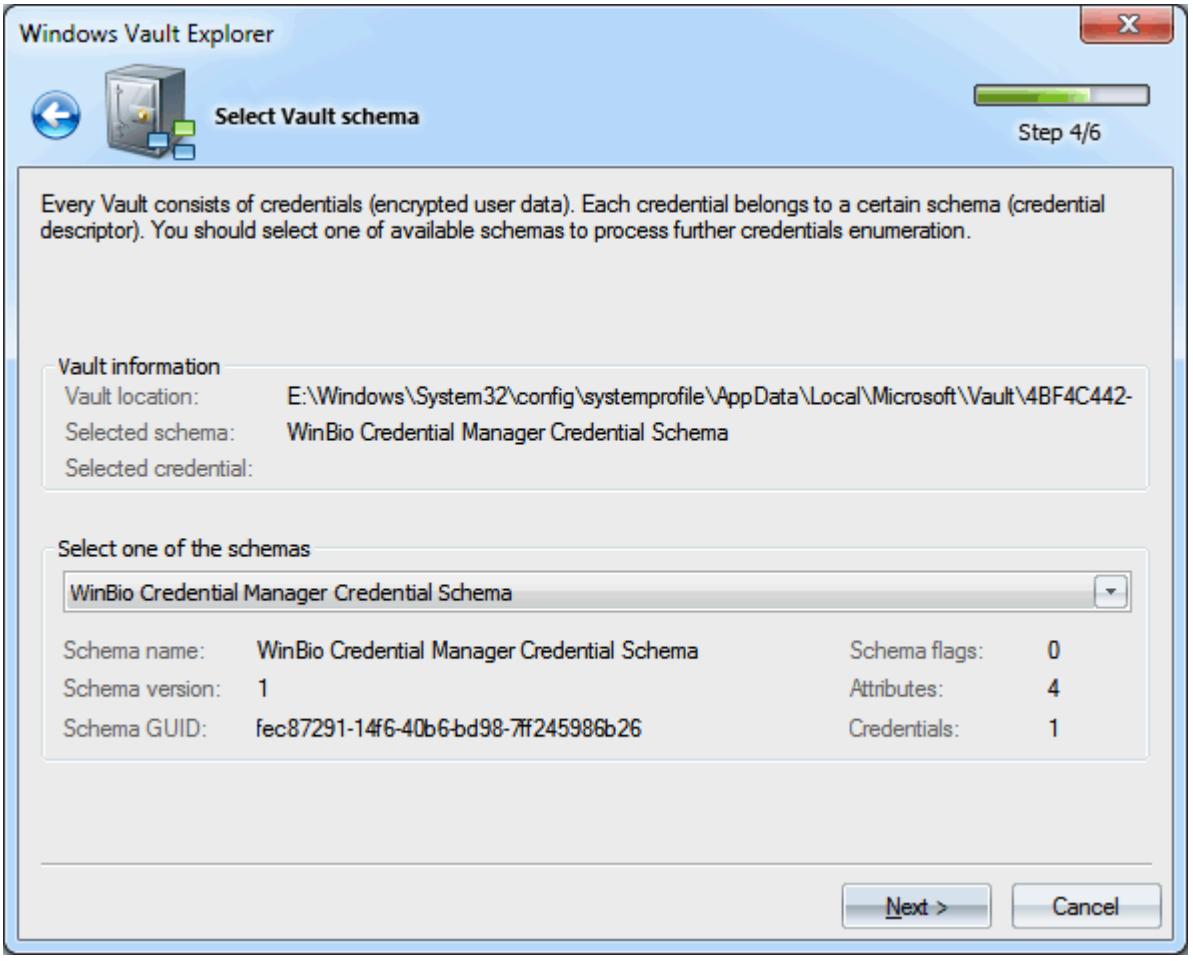
To decrypt a user's Master Key, you need to provide at least two parameters: the user's logon password and his security identifier (SID), which is normally included in the path to the Master Key. The program finds the user's SID automatically. If that hasn't been done for whatsoever reason, set it up manually. To decrypt the system's Master Key, we don't need to specify the password; the program will extract all the necessary information from the two registry files: **SYSTEM** and **SECURITY**.

In some cases, the decryption of the Master Key requires specifying the path to the **SAM** registry file. That's the case only when the account of the data owner in Windows 8 has the **LiveID** type.

Windows Password Recovery starting with version 9.7 uses some vulnerabilities in DPAPI Master Key encryption. Thus, to decrypt ANY Vault entry of a domain user, the owner logon password is not needed any longer.

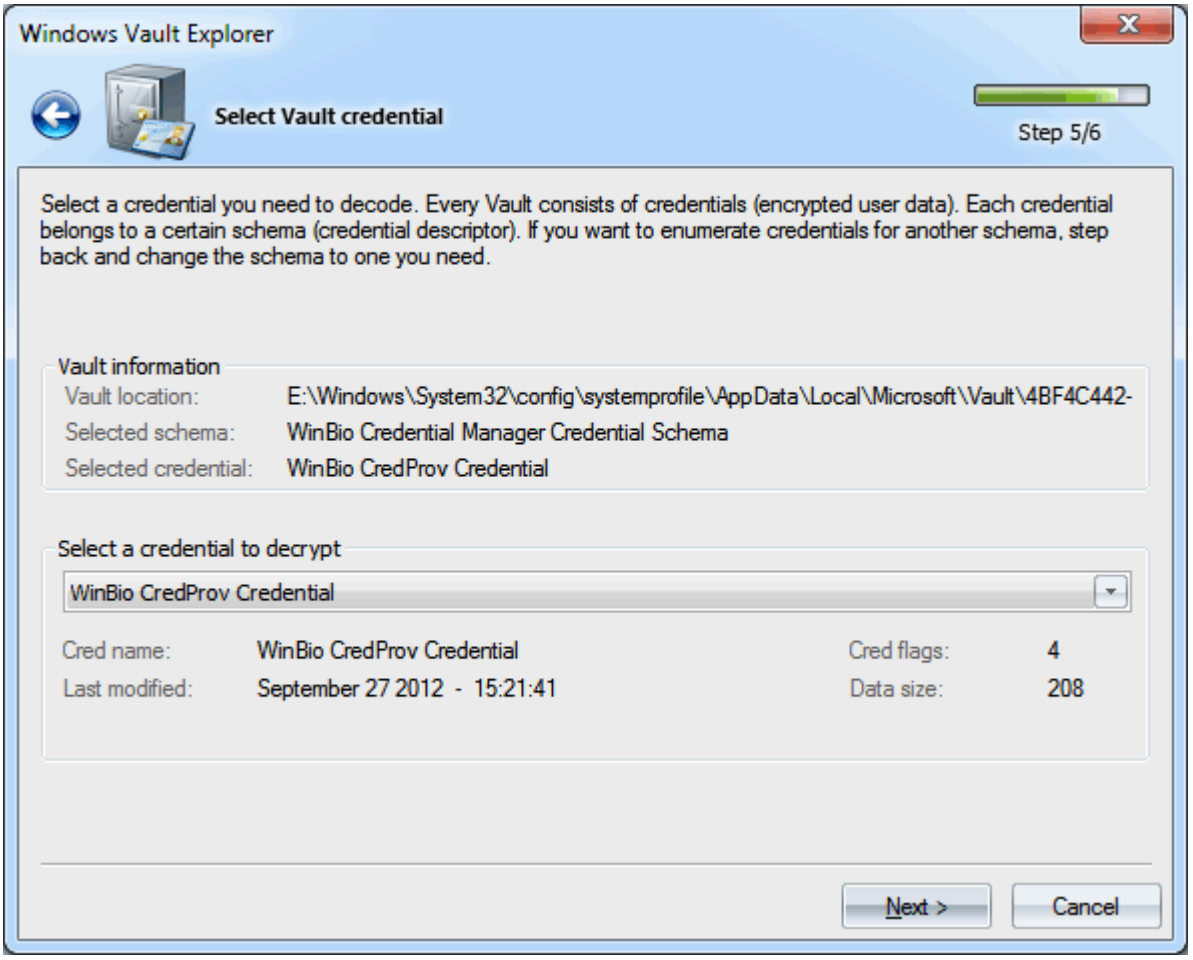
WPR v15 supports additional decryption methods using Windows Hello PIN or biometrics (password-less recovery).

Selecting Vault Schema



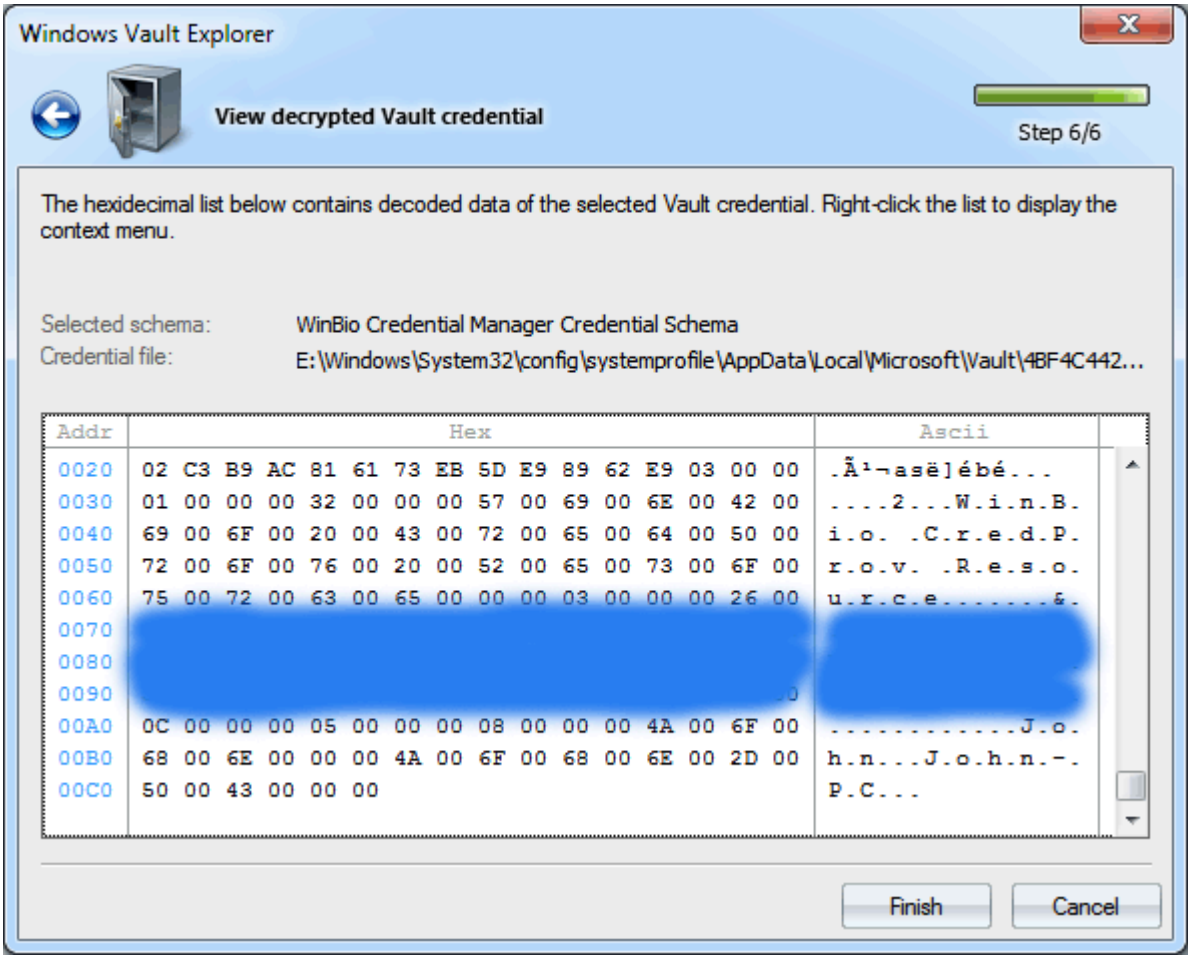
On the fourth step, if the previous ones passed successfully, the program prompts you to select one of the schemas belonging to our Vault from the dropdown list. Just below the list, we can see the general characteristics of the selected schema: its name, version, GUID, flags, number of attributes and credentials.

Selecting Vault credentials



In a similar manner, select one of the credentials of interest that belongs to the schema we have selected during the previous step.

Decrypting Vault credentials



And, at last, the final step, where you can view the decrypted record, copy it to clipboard or save to file for further analysis. The figure shows decrypted plain-text password (it is clobbered) of the administrator account configured to logon using biometric information (fingerprint).

Source: https://www.passcape.com/windows_password_recovery_vault_explorer