Credential history (CREDHIST) ahalysis

Section menu

- **Windows Passwords**
  - Reset Windows Password
  - Windows Password Recovery
    - Screenshots
    - Program FAQ
    - Windows passwords FAQ
    - GPU FAQ
    - Program versions
    - Registration
- **Password recovery for popular browsers**
- **Password recovery for e-mail clients**
- **Network passwords**
- **Office passwords**
- **Miscellaneous utilities**

23.10.2024
Reset Windows Password 15.0
Windows Phone Link forensics

10.10.2024
Wireless Password Recovery v6.10.2
Support for WPA-PSK AKM with SHA256 hashing

17.09.2024
Reset Windows Password v14.4
P2P network forensics

31.07.2024
Passcape ISO Burner v2.3.2
Some minor improvements and fixes

more news »

Articles and video

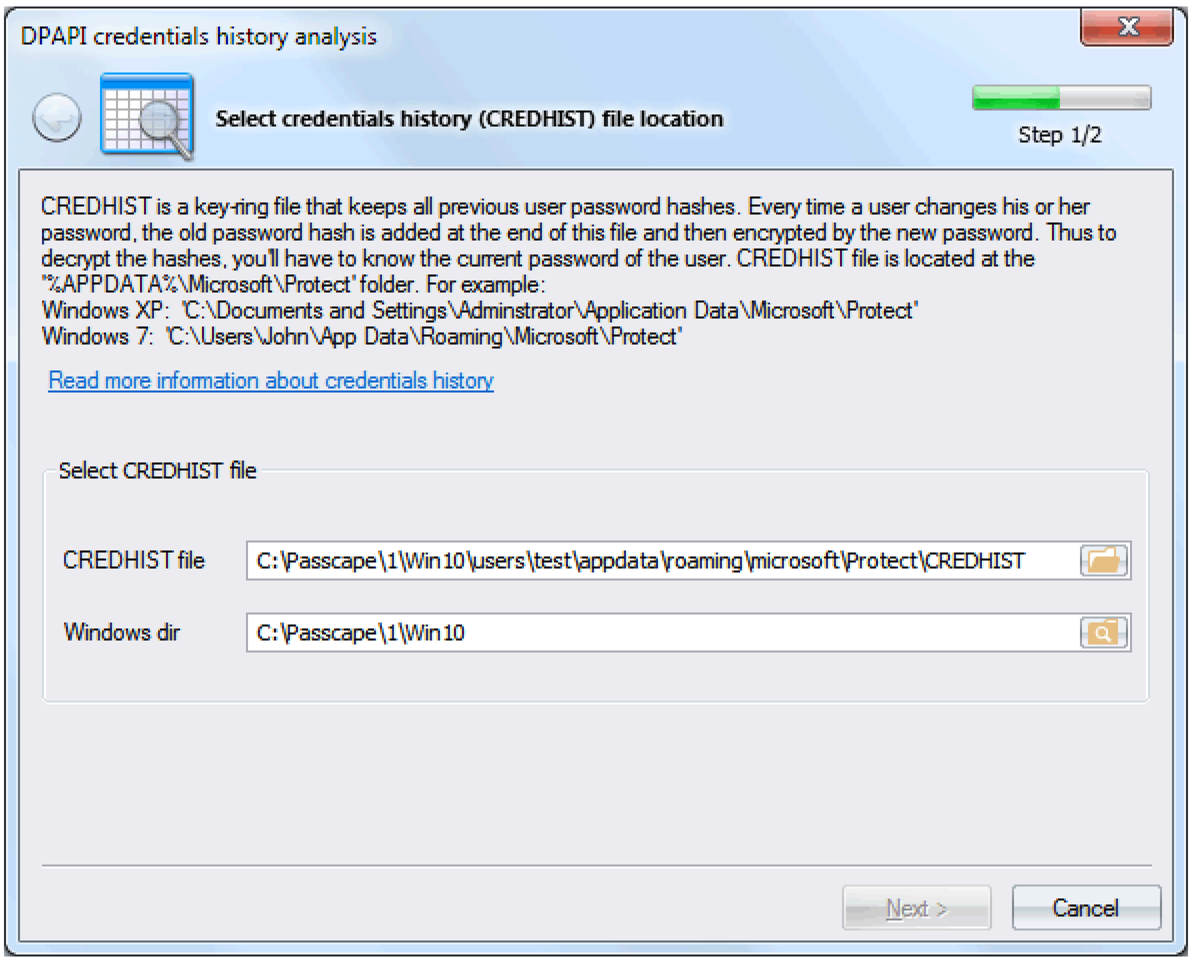
You may find it helpful to read our articles on Windows security and password recovery examples. Video section contains a number of movies about our programs in action

Windows Password Recovery - CREDHIST analysis

CREDHIST is a password history file, made out as a chain, where each link represents the user's older password hashes. Each time user changes the password, the old password hash is appended to the file and encrypted with a new password. Therefore, to decrypt all the hashes in a chain, you must know the user's current password.

Along with hashes, the chains store other service data, which is also analyzed by this utility.

Select CREDHIST file



CREDHIST is a key-ring file that keeps all previous user password hashes. Every time a user changes his or her password, the old password hash is added at the end of this file and then encrypted by the new password. Thus to decrypt the hashes, you'll have to know the current password of the user. CREDHIST file is located at the '%APPDATA%\Microsoft\Protect' folder. For example:
Windows XP: 'C:\Documents and Settings\Adminstrator\Application Data\Microsoft\Protect'
Windows 7: 'C:\Users\John\App Data\Roaming\Microsoft\Protect'

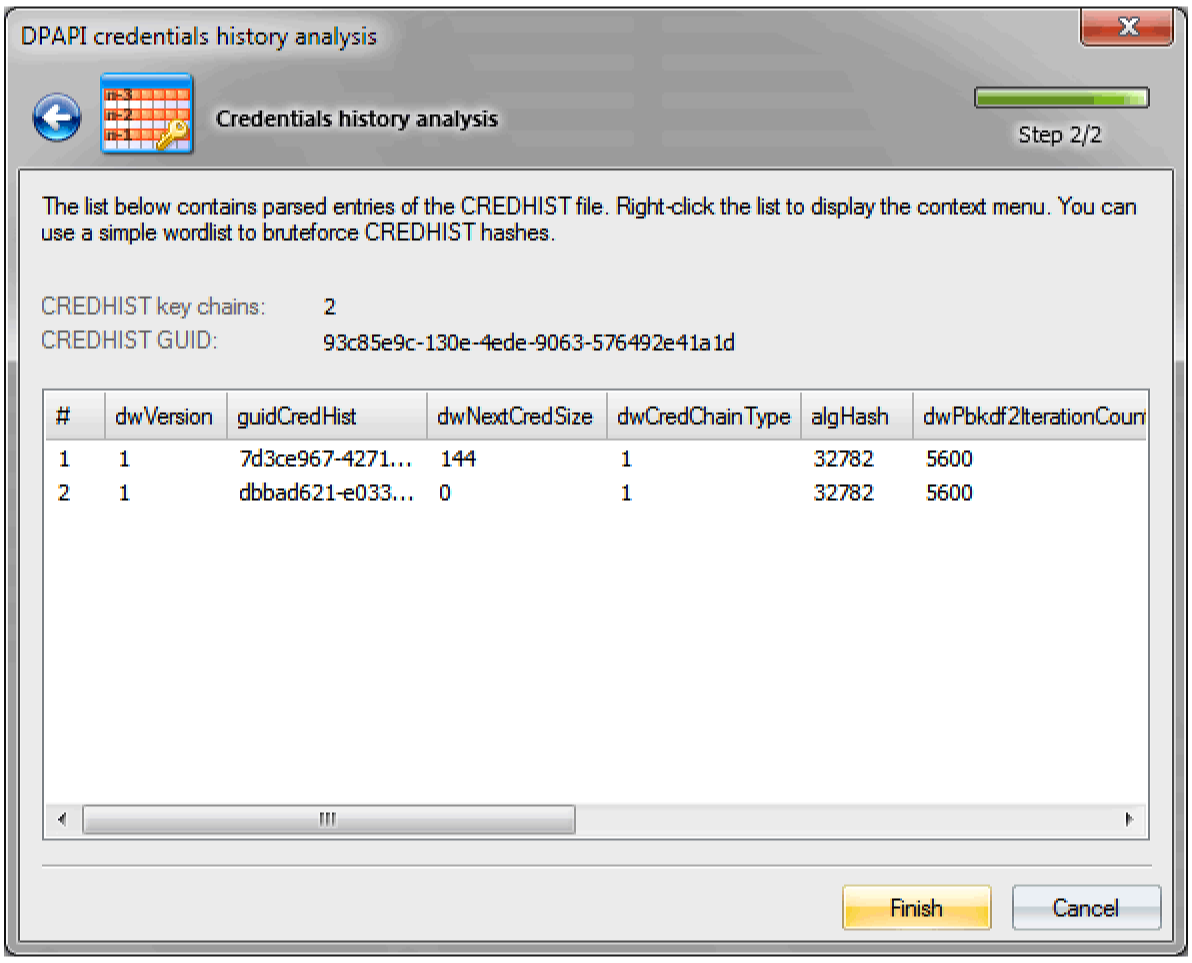
Read more information about credentials history

Select CREDHIST file

CREDHIST file: C:\Passcape\1\Win10\users\test\appdata\roaming\microsoft\Protect\CREDHIST

Windows dir: C:\Passcape\1\Win10

And proceed to analyze its content



The list below contains parsed entries of the CREDHIST file. Right-click the list to display the context menu. You can use a simple wordlist to bruteforce CREDHIST hashes.

CREDHIST key chains: 2
CREDHIST GUID: 93c85e9c-130e-4ede-9063-576492e41a1d

#	dwVersion	guidCredHist	dwNextCredSize	dwCredChainType	algHash	dwPbkdf2IterationCoun
1	1	7d3ce967-4271...	144	1	32782	5600
2	1	dbbad621-e033...	0	1	32782	5600

On the screenshot, you can see that the CREDHIST identifier is 93c85e9c-130e-4ede-9063-576492e41a1d. This is the identifier (GUID) all user's Master Keys in the context of the data owner are attached to. The number of links in the hash chain is 2.

The list below contains all attributes and their values for each link of our CREDHIST.

Attribute description

- ***dwVersion*** - data structure version
- ***guidCredHist*** - current link unique identifier
- ***dwNextCredSize*** - next link size
- ***dwCredChainType*** - link type
- ***algHash*** - hashing algorithm used when decrypting the link
- ***dwPbkdf2IterationCount*** - iterations in the PKCS#5 PBKDF2 key generation routine
- ***dwSidSize*** - owner security descriptor (SID) size
- ***algCrypt*** - encryption algorithm
- ***dwShaHashSize*** - SHA1 hash size
- ***dwNtHashSize*** - NTLM hash size
- ***pSalt*** - salt used in the encryption
- ***sidUser*** - data owner SID
- ***pShaHash*** - SHA1 hash
- ***pNtHash*** - NTLM hash

To guess the original CREDHIST password, right-click on the attributes and then select '*Use a dictionary to validate password...*' on the context menu that appears. You can validate the password or PIN for both currently selected and all the records. The validation time increases proportionally to the number of the records (i.e. links).

See the original CREDHIST password search speed comparative table. The speed is measured on a single-core Intel Q8400 CPU for default OS configurations (for example, in Windows 7, the number of iterations in PBKDF2 may differ).

Operating System	Encryption algorithm	Hash function	PBKDF2 counter	Password check speed (p/s)
Windows XP	3DES	SHA1	4000	**76**
Windows Vista	3DES	SHA1	24000	**12**
Windows 7	AES256	SHA512	5600	**10**
Windows 10-11	AES256	SHA512	8000	**7**