

## Password Secrets of Windows Applications

### Internet Browsers



#### Firefox

**Firefox** with version 3.5 and earlier stores the sign-on passwords in the '**signons.txt**' file located in its profile directory. With version 3.5 onwards Firefox started storing the sign-on passwords in Sqlite database file named '**signons.sqlite**'. The passwords stored in this sign-on file are encrypted using **Triple-DES** followed by **BASE64** encoding mechanism.

Here is the default location of Firefox profile directory,

```
[Windows XP]
C:\Documents and Settings\\Application
Data\Mozilla\Firefox\Profiles\.default

[Windows Vista & Windows 7]
C:\Users\\AppData\Roaming\Mozilla\Firefox\Profiles\.default
```

Firefox provides additional protection option called '**master password**' to prevent malicious users from discovering these sign-on passwords. Master password as such is not stored anywhere directly but its one way hash and other relevant information is stored in the key3.db file within the profile directory.



#### Flock

**Flock browser** uses similar storage format & encryption mechanism as Google Chrome.

It stores website login passwords in the **sqlite database** file called '**Login Data**' at following profile location.

```
[Windows XP]
C:\Documents and Settings\\Local Settings\Application Data\Flock\User
Data\Default

[Windows Vista & Windows 7]
C:\Users\\Appdata\Local\Flock\User Data\Default
```

Each stored sign-on entry mainly contains website URL, username field id, username, password field id and encrypted password.



## Google Chrome

**Google Chrome** stores all sign-on passwords in the **sqlite database** file called '**Web Data**' within the profile directory. Newer version uses '**Login Data**' file for storing login passwords. Here is the default location of Chrome profile directory.

```
[Windows XP]
C:\Documents and Settings\\Local Settings\Application
Data\Google\Chrome\User Data\Default

[Windows Vista & Windows 7]
C:\Users\\Appdata\Local\Google\Chrome\User Data\Default
```

Each stored sign-on entry mainly contains website URL, username field id, username, password field id and encrypted password.



## Google Chrome Canary or SXS

**Google Chrome Canary or SXS** is the parallel test version of Chrome which user can download and test, there by helping Google to release stable version of Chrome.

Like Chrome, it also stores all sign-on passwords in the **sqlite database** file called '**Web Data**' within the profile directory. Newer version uses '**Login Data**' file for storing login passwords. However profile location of Chrome Canary build is slightly different, here it is

```
[Windows XP]
C:\Documents and Settings\\Local Settings\Application
Data\Google\Chrome SXS\User Data\Default

[Windows Vista & Windows 7]
C:\Users\\Appdata\Local\Google\Chrome SXS\User Data\Default
```

Also it uses same storage and encryption mechanism as Chrome. Each stored sign-on entry mainly contains website URL, username field id, username, password field id and encrypted password.



## Internet Explorer

**Internet Explorer** stores two types of passwords, sign-on and **HTTP basic authentication** (generally proxy, router configuration) passwords. IE below version 7 stores both sign-on and HTTP basic authentication passwords in the secure location known as '**Protected Storage**' in the following registry location,

```
HKEY_CURRENT_USER\Software\Microsoft\Protected Storage System Provider
```

With version 7 onwards IE uses the new mechanism to store the sign-on passwords. The encrypted password for each website are stored along with **hash of the website URL** in the following registry location.

```
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage2
```

Also IE 7 onwards, HTTP basic authentication passwords are stored in the '**Credentials store**' at following location based on the operating system.

```
[Windows XP]
C:\Documents and Settings\[username]\Application Data\Microsoft\Credentials

[Windows Vista and Windows 7]
C:\Users\[username]\AppData\Roaming\Microsoft\Credentials
```



### Maxthon

**Maxthon** (version 3.1.7.1000] stores all the web login user accounts including passwords in the file "**MagicFill2.dat**" at below mentioned location

```
[Windows XP]
C:\Documents and Settings\\Application
Data\Maxthon3\Users\\MagicFill

[Windows Vista & Windows 7]
C:\Users\Administrator\AppData\Roaming\Maxthon3\Users\\MagicFill
```

This magic file is fully encrypted with unknown algorithm. We will update here as we decipher more information.



### Opera

**Opera** stores the login passwords in an encrypted format in the '**Magic Wand File**' called '**Wand.dat**' within its profile directory. This profile path is different for different versions of Opera as shown below.

```
For Opera Version 10 and above
[Windows NT/2K/2k3/XP]
C:\Documents and Settings\\Application Data\Opera\Opera\wand.dat

[Windows Vista/Windows 7]
C:\Users\\AppData\Roaming\Opera\Opera\wand.dat

For Opera Version less than 10
[Windows NT/2K/2k3/XP]
```

```
C:\Documents and Settings\\Application
Data\Opera\Opera\profile\wand.dat

[Windows Vista/Windows 7]
C:\Users\\AppData\Roaming\Opera\Opera\profile\wand.dat
```

Wand file mainly contains website URL, username and password information which are encrypted using **Triple-DES** algorithm.



## Safari

**Safari** uses strong storage format and encryption mechanism for securely storing website login passwords. Login passwords along with other information are stored in '**keychain.plist**' file at following central location.

```
[Windows XP]
C:\Documents and Settings\\Application Data\Apple Computer\Preferences

[Windows Vista & Windows 7]
C:\Users\\Appdata\AppData\Roaming\Apple Computer\Preferences
```

The Keychain file uses binary **Property List format** (typically found in MAC) which contains information such as website server name, user login & encrypted password. Password is encrypted using the **Cryptography functions** with the salt value to keep it stronger.

## Instant Messengers



### AIM (AOL Instant Messenger)

**AIM** version 6.x (till v7.2) onwards stores the password at the following registry location,

```
HKEY_CURRENT_USER\Software\America Online\AIM6\Passwords
```

AIM PRO version uses the different registry location to store the passwords,

```
HKEY_CURRENT_USER\Software\AIM\AIMPRO\
```

Latest version of **AIM (v7.5 since v7.3)** stores the encrypted username/password in the file '**aimx.bin**' at following location

```
[Windows XP]
C:\Documents and Settings\\Local Settings\Application Data\AIM
```

```
[Windows Vista & Windows 7]
C:\Users\\AppData\Local\AIM
```

AIM uses **Blowfish** encryption algorithm along with Base64 encoding to securely store the login passwords.



### **Beylux** Messenger

**Beylux** Messenger stores main account password at following registry location

```
HKEY_CURRENT_USER\Software\Beylux Messenger\
```

Password for each user is encrypted and stored in the registry value '**password**' under this key.



### **BigAnt** Messenger

**BigAnt** Messenger (version 2.82) stores the login name and password at following registry location,

```
HKEY_CURRENT_USER\Software\BigAntSoft\BigAntMessenger\Setting
```

Login name is stored in the registry value "**LoginName**" and encrypted password is stored in the registry value '**Password**' under this key.



### **Digsby**

Newer versions of **Digsby** (Build 83 - r27225 as of this writing) stores main account password in the '**logininfo.yaml**' file at following location,

```
[Windows XP]
C:\Documents and Settings\\Local Settings\Application Data\Digsby

[Windows Vista & Windows 7]
C:\Users\\AppData\Local\Digsby
```

Digsby stores only main account password locally and all other IM account passwords (such as Yahoo, Gmail, AIM) are stored in the servers. Main Digsby password is encrypted using special algorithm with username, windows product id, install date as key and resulting password is then encoded with **BASE64** before storing into the above password file.

Earlier versions of Digsby used to save the password in the '**Digsby.dat**' file at following location,

```
[Windows XP]
C:\Documents and Settings\\Application Data\Digsby

[Windows Vista & Windows 7]
C:\Users\\AppData\Roaming\Digsby
```

Earlier Digsby versions used hardcoded string '**foo**' as key without BASE64 encoding.



### Google Talk (GTalk)

**Google Talk** (GTalk) stores all remembered gmail account information at following registry location.

```
HKEY_CURRENT_USER\Software\Google\Google Talk\Accounts
```

For each **Google account** separate registry key is created with the account email id as name under this key. Account password is encrypted and stored in the registry string value named '**pw**' within this account **registry key**.



### IMVU Messenger

**IMVU Messenger** (version 450.2) stores the login account information at following registry location,

```
HKEY_CURRENT_USER\Software\IMVU\username  
HKEY_CURRENT_USER\Software\IMVU\password
```

Username is stored in clear text and **password** is stored in **hex format** as a default registry value.



### Meebo Notifier

**Meebo Notifier** (beta version) stores the login messenger account passwords in the '**MeeboAccounts.txt**' file at below mentioned location depending on your platform.

```
[Windows XP]  
C:\Documents and Settings\Application Data\Meebo\MeeboAccounts.txt  
  
[Windows Vista & Windows 7]  
C:\Users\AppData\Roaming\Meebo\MeeboAccounts.txt
```

This "MeeboAccounts.txt" file contains username in clear text and **login password** encoded with **magic bytes**.



### Miranda IM

**Miranda** is open source based popular messenger of recent times. Like most instant messengers, **Miranda** also stores the all user account information including passwords in the profile location. This is to prevent the user from entering the passwords each time.

Latest version of Miranda (**v0.9.10**) stores the user account & password in the profile file at following location

```
[Windows XP]  
C:\Documents and Settings\\Application  
Data\Miranda\%profile_name%\%profile_name%.dat
```

```
[Windows Vista & Windows 7]
```

```
C:\Users\\AppData\Roaming\Miranda\%profile_name%\%profile_name%.dat
```

User can have multiple profiles specific to office or home environment and corresponding account information is stored in the respective profile file.

Initial versions of Miranda stored all account information in .dat file directly within the base location as shown below,

```
[Windows XP]
```

```
C:\Documents and Settings\\Application Data\Miranda\.dat
```

```
[Windows Vista & Windows 7]
```

```
C:\Users\\AppData\Roaming\Miranda\.dat
```

Miranda uses its own proprietary mechanism to encrypt the password before storing into the profile file.



### MSN Messneger

**MSN Messenger** also uses '**Credential Store**' to securely store the remembered passwords. These passwords are stored as type '**Domain Visible Network**' aka '**.Net Passport**' using the target name as '.Net passport' within the 'Credential Store'.



### MySpace IM

**MySpaceIM** is one of the upcoming instant messenger which stores the user account & password details at following location.

```
[Windows XP]
```

```
C:\Documents and Settings\\Application Data\MySpace\IM\users.txt
```

```
[Windows Vista & Windows 7]
```

```
C:\Users\\AppData\Roaming\MySpace\IM\users.txt
```

The user login email id is stored in clear text where as the password is in encrypted format. The password is encrypted using '**Windows Crypto API**' functions and then encoded using **BASE64** algorithm before storing into this file. So in order to decrypt it successfully one has to decode the password using **BASE64** and then decrypt it using **CryptUnprotectData** function.



### Nimbuzz Messenger

**Nimbuzz Messenger** (version 1.6) stores the login account information at following registry location,

```
HKEY_CURRENT_USER\Software\Nimbuzz\PCClient\Application
```

It stores all the account details including login username & password (stored in hex format) in registry values "**username**" & "**password**" respectively.



### **PaltalkScene**

**PaltalkScene** stores main account password at following registry location

```
HKEY_CURRENT_USER\Software\Paltalk\<nick_name>
```

Password is encrypted and stored in the registry value '**pwd**' under this key. All other IM passwords such as Gmail, Yahoo, AIM etc are saved under separate sub keys under this registry key. For example Gmail accounts are stored under following registry key,

```
HKEY_CURRENT_USER\Software\Paltalk\<nick_name>\GGL\<gmail_address>
```

All these IM passwords are encoded with **BASE64** and stored in '**pwd**' registry value.



### **Pidgin (Formerly Gaim)**

**Pidgin** stores all configured account passwords in the "**Accounts.xml**" file located at following directory

```
[Windows XP]
C:\Documents and Settings\<user_name>\Application Data\.purple

[Windows Vista & Windows 7]
C:\Users\<username>\AppData\Roaming\.purple
```

Older versions (Gaim) used **.gaim folder** instead of .purple to store the account details. For each stored account, 'Accounts.xml' file contains the <account> tag, which has sub tags <name> & <password> containing the account email address and password in plain text respectively.



### **Skype**

**Skype** does not store password directly. Instead it stores the encrypted hash of the password in the '**config.xml**' located in Skype's user profile directory. Typical user profile directory for Skype will be as follows,

```
[Windows XP]
C:\Documents and Settings\<user_name>\Application Data\Skype\<account_name>

[Windows Vista & Windows 7]
C:\Users\<username>\AppData\Roaming\Skype\<account_name>
```

This config.xml contains **<Credentials2>** tag which contains encrypted hash of the password. As per the research paper '**Vanilla Skype**' written by Fabrice Desclaux and Kostya Kortchinsky, Skype uses the MD5 hash of string "**username\nskyper\npassword**" for authentication. If user has set the 'Remember password' option then this MD5 hash is encrypted using **AES-256 & SHA-1** algorithms and finally saved into the 'Config.xml' file.

Since the HASH of the password is saved, it is not possible to directly get the password. Instead one has to use dictionary or brute force approach to find out the right password from the hash. This approach may take days or months together based on the length & complexity of the password.



## Tencent QQ

**Tencent QQ** is one of the popular instant messenger which stores the user's login information in the file "**Registry.db**" at following location

```
C:\Users\\Documents\Tencent Files\
```

This "Registry.db" file is in the OLE storage format which can be viewed using DocFile Viewer. However internal login information is encrypted using **Blowfish** algorithm.



## Trillian

[**Version 4.21 build 24**] - [**Version 5.0.0.26**]

**Trillian Astra** stores only main account passwords (called as Identity or Astra password) in the '**accounts.ini**' file at below mentioned location. But all other IM account passwords (such as Yahoo, Gtalk, AIM, MSN etc) are stored on the servers.

```
[Windows XP]
C:\Documents and Settings\\Application Data\Trillian\users\global\

[Windows Vista & Windows 7]
C:\Users\\AppData\Roaming\Trillian\users\global\
```

For each account it contains section named "**[Account<number>]**" under which all information for that account is stored. Username is stored in the field named 'Account=' and password is stored in the field 'Password='. Trillian first performs **XOR encoding** of the password with standard pattern and then encodes it with **BASE64** before storing it.



## Windows Live Messenger

Windows Live Messenger stores the account password at '**Credential Store**' which provides different mechanisms such as 'Generic', 'Domain Network', 'Domain Visible Network' etc which applications can use to store and retrieve their private credentials. Each such method requires different technique and privilege level to enumerate and decrypt the passwords.

Windows Live Messenger uses '**Generic Password**' mechanism of 'Credential Store' to store the passwords under the target name '**WindowsLive:name=<email\_id>**'.



### Xfire

**Xfire** is a free tool that automatically keeps track of when and where gamers are playing games online with more than million members. Xfire stores the user settings including login username & password in a file "**XfireUser.ini**" at following location,

```
[Windows XP]
C:\Documents and Settings\\Application Data\Xfire

[Windows Vista & Windows 7]
C:\Users\\AppData\Roaming\Xfire\
```

Xfire uses **blowfish encryption** algorithm for both username & password. Each encrypted Username is stored with the label "**EncryptedUser1**" and password is stored as "**EPW1**". However Xfire does not store the original password directly. Instead it generates the SHA1 hash of **username+password+"UltimateArena"** and then store the encrypted data of this **SHA1 hash**.



### Yahoo Messenger

**Yahoo Messenger** prior to version 7 used to store the password in the registry value '**EOptions String**' at following registry location,

```
HKEY_CURRENT_USER\Software\Yahoo\Pager
```

This password is encrypted and then encoded using **Yahoo64** (similar to Base64) algorithm and stored at above location. The actual algorithm and encoding functionality is present in **ycrwin32.dll** (can be found in installed location of Yahoo Messenger).

For **version 7** onwards, Yahoo stores the encrypted token derived from username & password in **registry value 'ETS'** at same registry location. Though you **cannot decrypt** this token back to the password but you can copy it to another machine and continue to login to Yahoo Messenger.

## Email Client Applications



### Foxmail

**Foxmail** [version 6.5] stores all the configured mail account password information at following location,

```
[Windows - 32 bit]
C:\Program Files\Foxmail\mail\\Account.stg

[Windows - 64 bit]
C:\Program Files (x86)\Foxmail\mail\\Account.stg
```

This "**Account.stg**" file appears to be in binary format as first 0x800 bytes are filled with some hex data then follows the actual account information including POP3 and SMTP account passwords. POP3 & SMTP account passwords are stored by the name '**POP3Password**' & '**ESMTPPassword**' respectively. The passwords are stored in hex format and XOR encoded using the magic string "**~draGon~**".



### Gmail Notifier

Gmail Notifier uses different mechanism to store the Google account password based on IE versions. For IE version 7 onwards, Gmail Notifier stores the password in the 'Windows Credential Store'. This password can be decrypted using **CredEnumerate** API function.



### IncrediMail

**IncrediMail** stores all the configured mail account password information at following registry location,

```
HKEY_CURRENT_USER\Software\IncrediMail\Identities\{GUID_1}\Accounts\{GUID_2}
```

Main account details such as Email address, POP3 password, SMTP password are stored in registry values '**EmailAddress**', '**PopPassword**' & '**Smtppassword**' respectively. Passwords are encoded using magic byte pattern "**0x89, 0x32, 0xCA, 0x31**"



### Microsoft Outlook

Newer version of Outlook starting from 2002 to **latest version 2010**, store the passwords (other than exchange server) for various email account such as POP3, IMAP, SMTP, HTTP at following registry location.

```
[Windows NT onwards]
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging
Subsystem\Profiles

[Prior to Windows NT]
HKEY_CURRENT_USER\Software\Microsoft\Windows Messaging Subsystem\Profiles
```

Newer versions of Outlook from 2002-2010 stores the **Exchange server passwords** in '**Credential Store**' as it provides better protection over other methods. You can use OutlookPasswordDecryptor or NetworkPasswordDecryptor to recover such passwords.

Older versions of Outlook (**Outlook Express, 98, 2000** etc) stores the Email configuration information along with encrypted password at following registry location,

```
[For Outlook installed in Internet Mail Only Mode Configuration]
HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\OMI Account Manager\Accounts

[For Outlook in normal mode]
HKCU\Software\Microsoft\Internet Account Manager\Accounts
```



## ThunderBird

**ThunderBird** stores all remembered email settings along with password into the SQLite database file '**signons.sqlite**' in its profile location. The default profile location for different platforms is as follows,

```
[Windows XP]
C:\Documents and Settings\\Application
Data\Thunderbird\Profiles\.default

[Windows Vista & Windows 7]
C:\Users\\AppData\Roaming\Thunderbird\Profiles\.default
```

## FTP Client Applications



## Dreamweaver

**Dreamweaver** - popular web site editing software - stores FTP & WebDav login & password information in the registry at following location.

```
HKEY_CURRENT_USER\Software\Adobe\Common\10\Sites\~SiteX\Keychain
```

For **Dreamweaver CS5** edition, replace 10 with 11 in above location. Each FTP site entry is stored in separate key "-SiteX" (as shown above) where X starts with 1 and incremented for every new FTP site. Each such Keychain entry contains user and encrypted password stored within the registry values named "**User**" & "**User PW**" respectively.

Dreamweaver uses the standard **Windows Cryptography Functions (CryptProtectData)** to encrypt the password before saving it to registry.



## FileZilla

**FileZilla** stores all account information along with username & password in the "**recentervers.xml**" file at following location,

```
[Windows XP]
C:\Documents and Settings\\Application Data\FileZilla
```

```
[Windows Vista & Windows 7]
C:\Users\\AppData\Roaming\FileZilla
```

This xml file contains entry for each ftp server account with tag <server>. For each server entry, there is <user> & <pass> tags which contains user name & password in **plain text** for corresponding FTP server.



### FlashFXP

**FlashFXP** - one of the emerging FTP clients - stores FTP login & password information in '**Sites.dat**' file at below location,

```
[Windows XP]
C:\Documents and Settings\All Users\Application Data\FlashFXP\4\Sites.dat
```

```
[Windows Vista & Windows 7]
C:\ProgramData\FlashFXP\4\Sites.dat
```

The above location applies to FlashFXP v4 or higher. For version 3 replace 4 with 3 in the above location. FlashFXP uses simple encoding algorithm with magic string as "**yA36zA48dEhfrvghGRg57h5UIDv3**" to encrypt the password.



### FTPCommander

**FTPCommander** one of the popular FTP clients which comes in FREE, Pro & Deluxe editions.

FTPCommander FREE edition stores the FTP site information in a file "**Ftplist.txt**" at its installed location

```
[Windows - 32 bit]
C:\Program Files\FTP Commander
```

```
[Windows - 64 bit]
C:\Program Files (x86)\FTP Commander
```

**FTPCommander PRO** edition stores the FTP site information in a file "Ftplist.txt" at following location

```
[Windows - all platforms]
C:\CFtp\
```

**FTPCommander Deluxe** edition stores the FTP site information in a file "Ftplist.txt" at its installed location

```
[Windows - 32 bit]
C:\Program Files\FTP Commander Deluxe
```

```
[Windows - 64 bit]
C:\Program Files (x86)\FTP Commander Deluxe
```

All editions for FTPCommander (as of latest version v9.2) stores the password along with server & username after performing **XOR encoding** of the password with **magic number 0x19 (25)**.



## SmartFTP

**SmartFTP** - one of the popular commercial FTP client - stores all the configured FTP account & password information at following location

```
[Windows XP]
C:\Documents and Settings\\Application Data\SmartFTP\Client
2.0\Favorites\Quick Connect

[Windows Vista & Windows 7]
C:\Users\\AppData\Roaming\SmartFTP\Client 2.0\Favorites\Quick Connect
```

SmartFTP (as of latest version v4.0) stores each FTP site information (host, username & password) in **separate XML file** in the above location. Password is encrypted using the '**Windows Cryptography Functions' (CryptEncrypt)**. It uses the RC4 encryption algorithm with the key derived from MD5 hash of **magic string "SmartFTP"**.



## WS\_FTP

**WS\_FTP** - one of the popular FTP client - stores all the configured FTP account & password information in the file "**ws\_ftp.ini**" at following location

```
[Windows XP]
C:\Documents and Settings\\Application Data\Ipswitch\WS_FTP\Sites\

[Windows Vista & Windows 7]
C:\Users\\AppData\Roaming\Ipswitch\WS_FTP\Sites\
```

Username and password for each of the stored FTP site is present after fields "uid=" and "pwd=" respectively. Password is encrypted using **Triple DES** algorithm with magic key and then stored in the **Base64** format.

## Miscellaneous Applications



### Google Desktop Search

'**Google Desktop Search**' stores the Google account information in the registry when it is configured to search your Gmail account. Here is the registry location,

```
HKEY_CURRENT_USER\Software\Google\Google Desktop\Mailboxes\Gmail
```

The above registry key contains the 2 main registry values, '**POP3\_name**' & '**POP3\_credentials**' holding the Google account name & encrypted password respectively.



### Heroes of Newerth

**Heroes of Newerth** (HoN) is popular game based on Warcraft III DoTA. It stored the user's login information in the file "**login.cfg**" at below location based on platform,

```
[Windows]
C:\Users\User\Documents\Heroes of Newerth\game\

[Linux]
/home/user/.Heroes of Newerth/game/

[Mac]
/Users/User/Library/Application Support/Heroes of Newerth/game/
```

This "login.cfg" file contains the username and password after the fields 'login\_name' & 'login\_password' respectively. Password field is nothing but **md5 hash** of the original password, which can be cracked using online **MD5 hash crackers** or offline tools.



### Internet Download Manager (IDM)

**IDM** stores all the premium account passwords for download sites at following registry location,

```
HKEY_CURRENT_USER\Software\DownloadManager\Passwords
```

There is registry key representing each download site below this location. Each such entry has 2 registry values "**User**" & "**EncPassword**". User name is the hex representation of ascii character, however password is **XOR encoded with 0xf**.



### JDownloader

**JDownloader** stores all the premium account passwords in the HSQL database file at following location,

```
[32 bit - x86 System]
C:\Program Files\JDownloader\Config
```

```
[64 bit - x64 System]
C:\Program Files (x86)\JDownloader\Config
```

**HSQldb** stores the database contents in terms of plain SQL statements. You can find all JDownloader configuration along with premium passwords in "**database.script**" file. There is no encryption as such but data itself is stored in serialized object format.



### Orbit Downloader

'**Orbit Downloader**' stores all the premium account passwords for download sites at following file,

```
[Windows XP]
C:\Documents and Settings\\Application Data\Orbit\sitelogin.dat

[Windows Vista & Windows 7]
C:\Users\\AppData\Roaming\Orbit\sitelogin.dat
```

The "**sitelogin.dat**" file contains website, username & password information for each of the premium download site. Passwords are encrypted using **IDEA algorithm**.



### Picasa

**Picasa** stores Google account password information at one of the following registry location.

```
HKEY_CURRENT_USER\Software\Google\Picasa\Picasa2\Preferences
HKEY_CURRENT_USER\Software\Google\Picasa\Picasa3\Preferences
```

Some of the early releases of Picasa 3 version used second location, but later switched back to previous location itself. The registry value '**gaiaEmail**' contains the Google account id and '**gaiaPass**' contains the encrypted password. Picasa versions 2 and 3 uses different encryption mechanisms to store the password.



### Remote Desktop

**Remote Desktop** stores the saved credentials at '**Credential Store**' using the target name as '**LegacyGeneric:target=TERMSRV/<Host\_IP\_address>**'. As many applications use 'Credential Store' to save their passwords, this target name can be used to uniquely identify 'Remote Desktop' stored passwords.



### TweetDeck

**TweetDeck** is the one of the popular Twitter client which also support other social networking sites such as Facebook, LinkedIn, MySpace, Buzz etc. It is developed using **Adobe Air** framework and hence it uses '**Encrypted Local Storage**' (ELS) mechanism provided by **Adobe Air** to store all the account credentials. The encrypted password files are stored at following location based on the platform,

```
[Windows XP]
C:\Documents and Settings\\Application
Data\Adobe\AIR\ELS\TweetDeckFast.FFF259DC0CE2657847BBB4AFF0E62062EFC56543.1
```

```
[Windows Vista & Windows 7]
C:\Users\\AppData\Roaming\Adobe\AIR\ELS\TweetDeckFast.FFF259DC0CE26578
47BBB4AFF0E62062EFC56543.1
```

On Windows, Adobe AIR uses **DPAPI functions** to encrypt the credentials using the 128 bit **AES-CBC** algorithm. Here is the typical sequence which is generally used to store the secret data.

```
var strToEncrypt:String = "passw0rd";

var myByteArray:ByteArray = new ByteArray();

myByteArray.writeUTFBytes(strToEncrypt);

EncryptedLocalStore.setItem("securityxploded", myByteArray);
```

I am still researching on to recover the account passwords stored by TweetDeck. I will update here as I discover more secrets.