



Introducing

SQUID

A tool to “fuzzy match” SQLite
databases

By Ryan Benson

About Me

Ryan Benson

DFIR @ Stroz Friedberg



@_RyanBenson



<https://github.com/obsidianforensics>



<http://www.obsidianforensics.com>



Self contained
database system, all
inside one file*

Used by:

- Google Chrome
- Skype
- Mozilla Firefox
- and many more...



DNA



SQLite



- Self-contained; where it came from doesn't matter
- Can be used to determine “relatives”
- Only a small portion of the sample is used

SQUID (SQLite Unknown IDentifier)

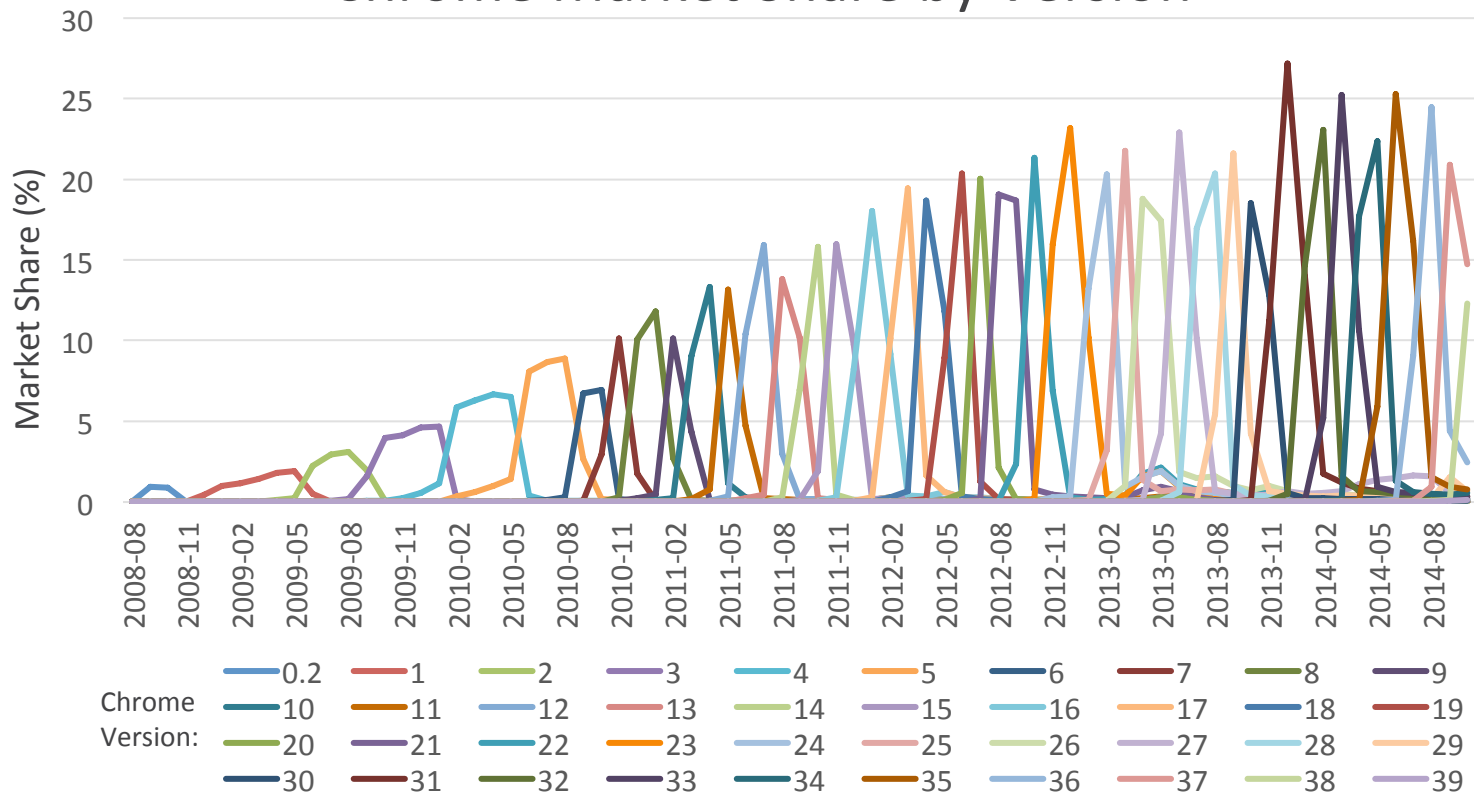
- Compares candidate against catalog of knowns
- Computes a comparison score between the two SQLite databases
 - Only looks at internal structure
 - Converted to percentage
- Allows for exact and partial matches

Frequent Updates to Applications

- Many modern apps get updated very frequently (much more frequently than many forensic tools)
- Changes can break analysis tools (or even worse, give incorrect results)



Chrome Market Share by Version



Points System

- Each matching table is 12 points
- Each matching column in a table is 6 points
- Each matching attribute of a column is 1 point (total of 3 attributes)
 - Type, Default Value, and Not Null
- Score is candidate / known, always ≤ 1

Points System

Candidate

| visits | | | |
|-------------|---------|---------------|----------|
| Column Name | Type | Default Value | Not Null |
| url | VARCHAR | "" | X |
| time | INT | 0 | X |
| expires | INT | 1 | |

Known

| visits | | | |
|-------------|---------|---------------|----------|
| Column Name | Type | Default Value | Not Null |
| url | VARCHAR | "" | X |
| time | INT | 0 | X |
| expires | INT | 0 | |
| icon | BLOB | | |

Points System

Candidate 12

| visits | | | |
|-------------|---------|---------------|----------|
| Column Name | Type | Default Value | Not Null |
| url | VARCHAR | "" | X |
| time | INT | 0 | X |
| expires | INT | 1 | |

Known 12

| visits | | | |
|-------------|---------|---------------|----------|
| Column Name | Type | Default Value | Not Null |
| url | VARCHAR | "" | X |
| time | INT | 0 | X |
| expires | INT | 0 | |
| icon | BLOB | | |

Points System

Candidate 18

| visits | | | |
|-------------|---------|---------------|----------|
| Column Name | Type | Default Value | Not Null |
| url | VARCHAR | "" | X |
| time | INT | 0 | X |
| expires | INT | 1 | |

Known 18

| visits | | | |
|-------------|---------|---------------|----------|
| Column Name | Type | Default Value | Not Null |
| url | VARCHAR | "" | X |
| time | INT | 0 | X |
| expires | INT | 0 | |
| icon | BLOB | | |

Points System

Candidate 21

| visits | | | |
|-------------|---------|---------------|----------|
| Column Name | Type | Default Value | Not Null |
| url | VARCHAR | "" | X |
| time | INT | 0 | X |
| expires | INT | 1 | |

Known 21

| visits | | | |
|-------------|---------|---------------|----------|
| Column Name | Type | Default Value | Not Null |
| url | VARCHAR | "" | X |
| time | INT | 0 | X |
| expires | INT | 0 | |
| icon | BLOB | | |

Points System

Candidate 30

| visits | | | |
|-------------|---------|---------------|----------|
| Column Name | Type | Default Value | Not Null |
| url | VARCHAR | "" | X |
| time | INT | 0 | X |
| expires | INT | 1 | |

Known 30

| visits | | | |
|-------------|---------|---------------|----------|
| Column Name | Type | Default Value | Not Null |
| url | VARCHAR | "" | X |
| time | INT | 0 | X |
| expires | INT | 0 | |
| icon | BLOB | | |

Points System

Candidate 36

| visits | | | |
|-------------|---------|---------------|----------|
| Column Name | Type | Default Value | Not Null |
| url | VARCHAR | "" | X |
| time | INT | 0 | X |
| expires | INT | 1 | |

Known 36

| visits | | | |
|-------------|---------|---------------|----------|
| Column Name | Type | Default Value | Not Null |
| url | VARCHAR | "" | X |
| time | INT | 0 | X |
| expires | INT | 0 | |
| icon | BLOB | | |

Points System

Candidate 38

| visits | | | |
|-------------|---------|---------------|----------|
| Column Name | Type | Default Value | Not Null |
| url | VARCHAR | "" | X |
| time | INT | 0 | X |
| expires | INT | 1 | |

Known 39

| visits | | | |
|-------------|---------|---------------|----------|
| Column Name | Type | Default Value | Not Null |
| url | VARCHAR | "" | X |
| time | INT | 0 | X |
| expires | INT | 0 | |
| icon | BLOB | | |

Points System

Candidate 38

| visits | | | |
|-------------|---------|---------------|----------|
| Column Name | Type | Default Value | Not Null |
| url | VARCHAR | "" | X |
| time | INT | 0 | X |
| expires | INT | 1 | |

Known 48

| visits | | | |
|-------------|---------|---------------|----------|
| Column Name | Type | Default Value | Not Null |
| url | VARCHAR | "" | X |
| time | INT | 0 | X |
| expires | INT | 0 | |
| icon | BLOB | | |

Points System

Candidate 38

79%

Known 48

visits

| Column Name | Type | Default Value | Not Null |
|-------------|---------|---------------|----------|
| url | VARCHAR | "" | X |
| time | INT | 0 | X |
| expires | INT | 1 | |

visits

| Column Name | Type | Default Value | Not Null |
|-------------|---------|---------------|----------|
| url | VARCHAR | "" | X |
| time | INT | 0 | X |
| expires | INT | 0 | |
| icon | BLOB | | |

Components

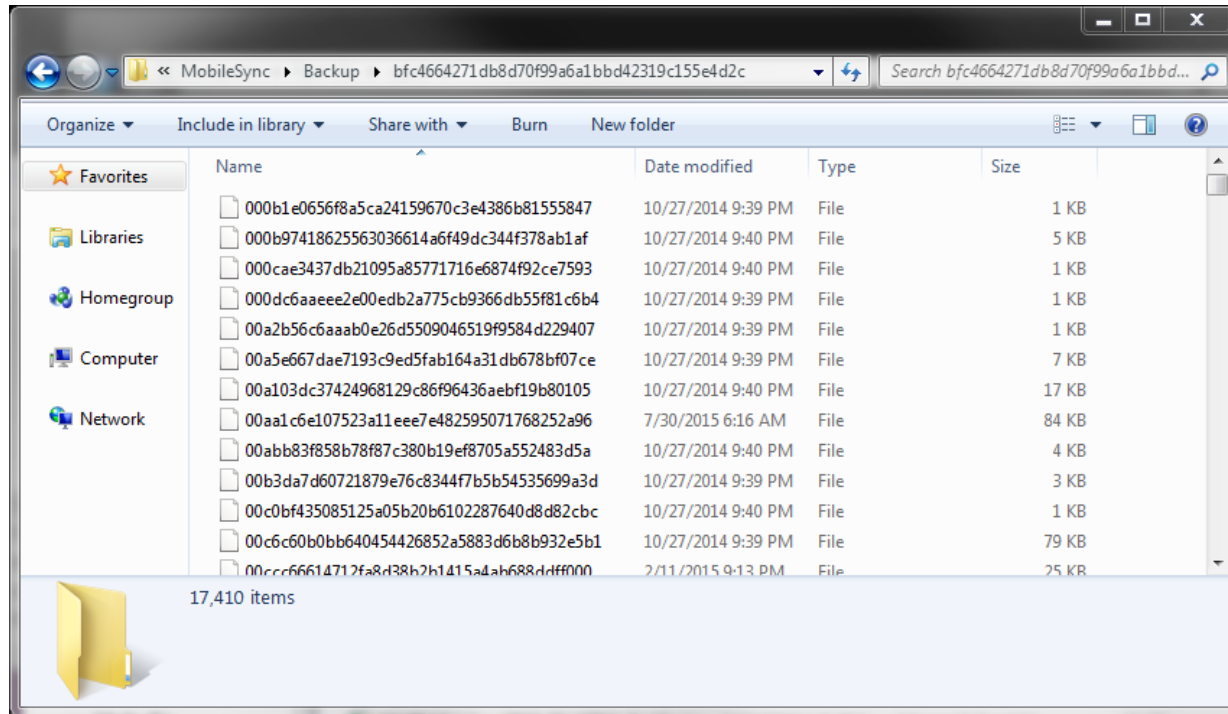


- Python script (squid.py)
- Catalog of 'known' databases

Comparison Commands

- Compare a file or directory using --compare or -c
 - Name the output report (XLSX) with --output or -o
- ```
> squid.py --compare F:\path\to\SQLite\files
--output "E:\Reports\SQUID_Report"
```

# Use Case #1: Phone Backups



# Use Case #1: Phone Backups

```
C:\Windows\system32\CMD.exe - squid.py --compare "C:\Users\Ryan\AppData\Roaming\Apple Computer\MobileSync\Backup\bfc4664271db8d70f99a6a1bbd42319c155e4d2c" --output "Ryan iPhone Backup"
```

S:\> squid.py --compare "C:\Users\Ryan\AppData\Roaming\Apple Computer\MobileSync\Backup\bfc4664271db8d70f99a6a1bbd42319c155e4d2c" --output "Ryan iPhone Backup"

-----

SQUID v0.4.0 - SQLite Unknown Identifier

-----

Scanning C:\Users\Ryan\AppData\Roaming\Apple Computer\MobileSync\Backup\bfc4664271db8d70f99a6a1bbd42319c155e4d2c and any subdirectories for SQLite DBs.

Below are any high-confidence (90+%) matches; a complete list of the top three matches for each SQLite DB is in "Ryan iPhone Backup.xlsx".

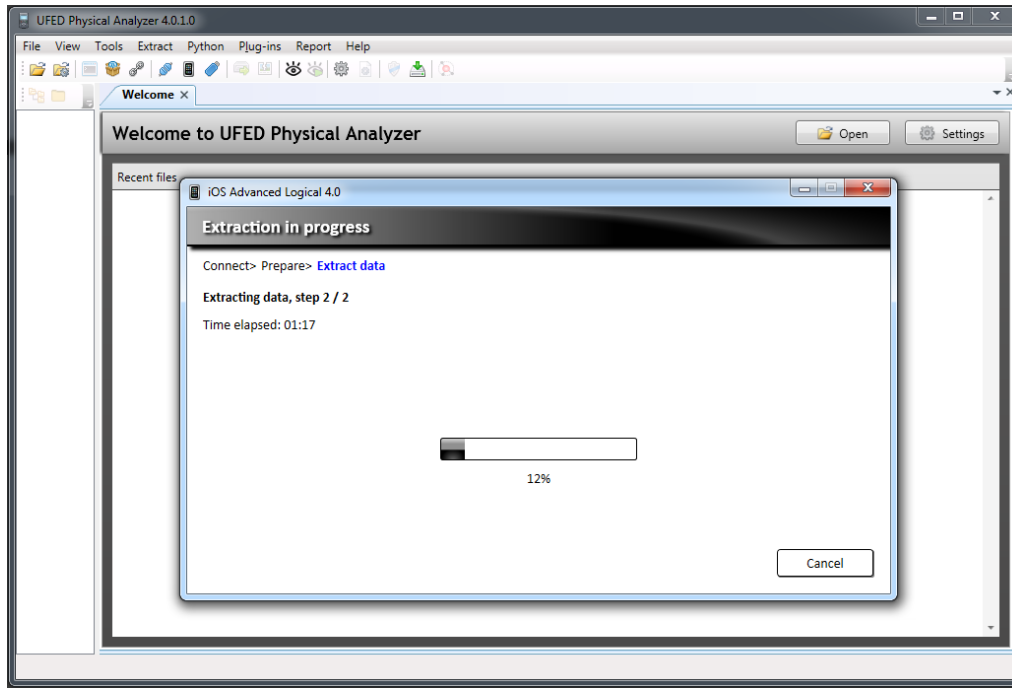
-----

| Candidate SQLite DB        | Match% | Known DB Name               | Known Program     |
|----------------------------|--------|-----------------------------|-------------------|
| 016b180b0173f6a618ba05f..  | 100.0% | googleanalytics-v3.sql      | Google Analytics  |
| 027cbce3ae649b49bfda37e..  | 97.8%  | business.sqlite             | Yelp              |
| 06196a61cf209070363f0b0..  | 100.0% | com.apple.MobileBluetooth.. | Bluetooth Devices |
| 12b144c0bd44f2b3dfffd918.. | 100.0% | Photos.sqlite               | Photos            |
| 14d1b8e008b39c2faf33ba4..  | 100.0% | googleanalytics-v2.sql      | Google Analytics  |
| 19f7d4cb78c336dbb4b5ce6..  | 100.0% | googleanalytics-v2.sql      | Google Analytics  |

# Use Case #1: Phone Backups

|     | A                          | B                                   | C      | D                  | E             | F       | G           |
|-----|----------------------------|-------------------------------------|--------|--------------------|---------------|---------|-------------|
| 1   | SQUID (v0.4.0)             |                                     |        |                    |               |         |             |
| 2   | Name                       | Path                                | Match  | DB Name            | Program Name  | Version | Category    |
| 60  | 55680ab883d0fdcfd94f959b1  | C:\Users\Ryan\AppData\Roaming\Apple | 100.0% | Favicons           | Google Chrome | 44 - 45 | Web Browser |
| 89  | 71e79b23acb72ba5a27912bdc  | C:\Users\Ryan\AppData\Roaming\Apple | 98.8%  | Cookies            | Google Chrome | 45      | Web Browser |
| 115 | 969ee001f767b7e12e58dfc57  | C:\Users\Ryan\AppData\Roaming\Apple | 100.0% | Origin Bound Certs | Google Chrome | 45      | Web Browser |
| 143 | caf47e54e28f38c93a994ce7e5 | C:\Users\Ryan\AppData\Roaming\Apple | 96.6%  | Web Data           | Google Chrome | 44 - 45 | Web Browser |
| 174 | eca153e5b0158cc8dcb805d7c  | C:\Users\Ryan\AppData\Roaming\Apple | 100.0% | Login Data         | Google Chrome | 44 - 45 | Web Browser |
| 178 | ef39c265a26270e9a4ffb6c487 | C:\Users\Ryan\AppData\Roaming\Apple | 100.0% | Top Sites          | Google Chrome | 32 - 45 | Web Browser |
| 186 | faf971ce92c3ac508c018dce1b | C:\Users\Ryan\AppData\Roaming\Apple | 97.7%  | History            | Google Chrome | 37 - 45 | Web Browser |
| 188 | fd304ca1dce131eede7df586d  | C:\Users\Ryan\AppData\Roaming\Apple | 100.0% | Shortcuts          | Google Chrome | 38      | Web Browser |

# Use Case #2: Second Opinion



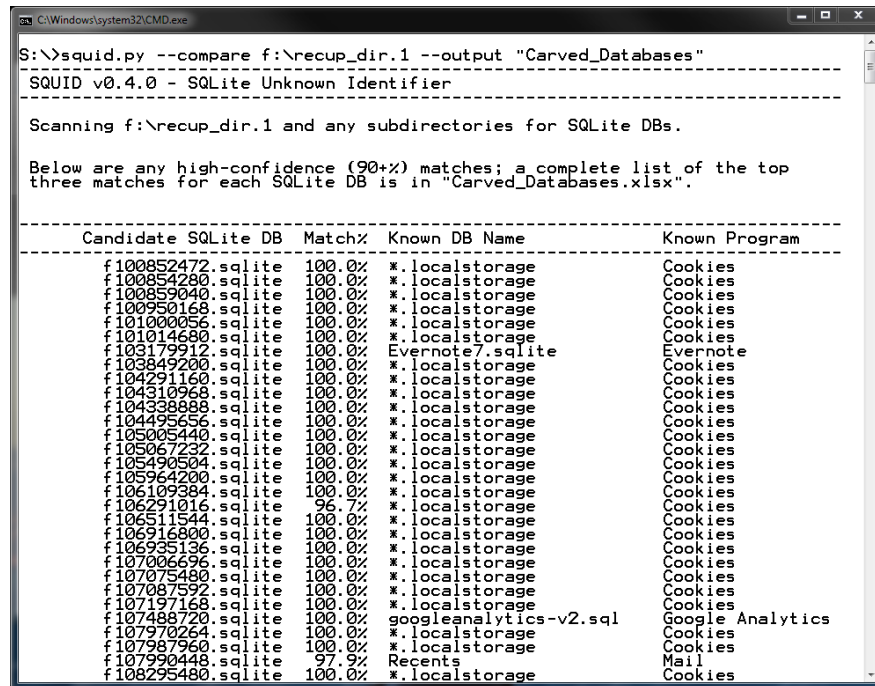


# Use Case #3: Carving from Windows

- Searched unallocated space on OS drive from Windows computer for SQLite files

```
> squid.py --compare "F:\recup_dir.1"
```

- Or live file system



```
C:\Windows\system32\CMD.exe
S:\>squid.py --compare f:\recup_dir.1 --output "Carved_Databases"

SQUID v0.4.0 - SQLite Unknown Identifier

Scanning f:\recup_dir.1 and any subdirectories for SQLite DBs.

Below are any high-confidence (90+%) matches; a complete list of the top
three matches for each SQLite DB is in "Carved_Databases.xlsx".

Candidate SQLite DB Match% Known DB Name Known Program

f100852472.sqlite 100.0% *.localstorage Cookies
f100854280.sqlite 100.0% *.localstorage Cookies
f100859040.sqlite 100.0% *.localstorage Cookies
f100950168.sqlite 100.0% *.localstorage Cookies
f101000366.sqlite 100.0% *.localstorage Cookies
f101014680.sqlite 100.0% *.localstorage Cookies
f103179912.sqlite 100.0% Evernote7.sqlite Evernote
f103849200.sqlite 100.0% *.localstorage Cookies
f104291160.sqlite 100.0% *.localstorage Cookies
f104310968.sqlite 100.0% *.localstorage Cookies
f104338888.sqlite 100.0% *.localstorage Cookies
f104495656.sqlite 100.0% *.localstorage Cookies
f105005440.sqlite 100.0% *.localstorage Cookies
f105067232.sqlite 100.0% *.localstorage Cookies
f105490504.sqlite 100.0% *.localstorage Cookies
f105964200.sqlite 100.0% *.localstorage Cookies
f106109384.sqlite 100.0% *.localstorage Cookies
f106291016.sqlite 96.7% *.localstorage Cookies
f106511544.sqlite 100.0% *.localstorage Cookies
f106916800.sqlite 100.0% *.localstorage Cookies
f106935136.sqlite 100.0% *.localstorage Cookies
f107006696.sqlite 100.0% *.localstorage Cookies
f107075480.sqlite 100.0% *.localstorage Cookies
f107087592.sqlite 100.0% *.localstorage Cookies
f107197168.sqlite 100.0% *.localstorage Cookies
f107488720.sqlite 100.0% googleanalytics-v2.sql Google Analytics
f107970264.sqlite 100.0% *.localstorage Cookies
f107987960.sqlite 100.0% *.localstorage Cookies
f107990448.sqlite 97.9% Recents Mail
f108295480.sqlite 100.0% *.localstorage Cookies
```

# Learning Commands

- Teach SQUID a new database using --learn or -l
- Specify details about the program the database is associated with using additional flags (--name, --family, --program, and --version)

```
> squid.py --learn "C:\Users\Ryan\AppData
\Local\Google\ Chrome\User Data\Default" --
program "Google Chrome" --version "46" --
family "Web Browser"
```

# SQUID: What's Next

- Keep building a bigger set of 'knowns'
- ESE DBs!
- Continue to tweak comparison algorithm (edit distance)
- Save queries in catalog to pull useful information from each 'known' database when found
- Simple GUI

# Questions?

4n6.link/squid



@\_RyanBenson



<https://github.com/obsidianforensics/squid>



<http://www.obsidianforensics.com>