Introducing

SQUID

A tool to “fuzzy match” SQLite databases

By Ryan Benson

STROZ FRIEDBERG

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…


CSI:
CRIME SCENE
INVESTIGATION
WWW.ENTERTAINMENTWALLPAPER.COM

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

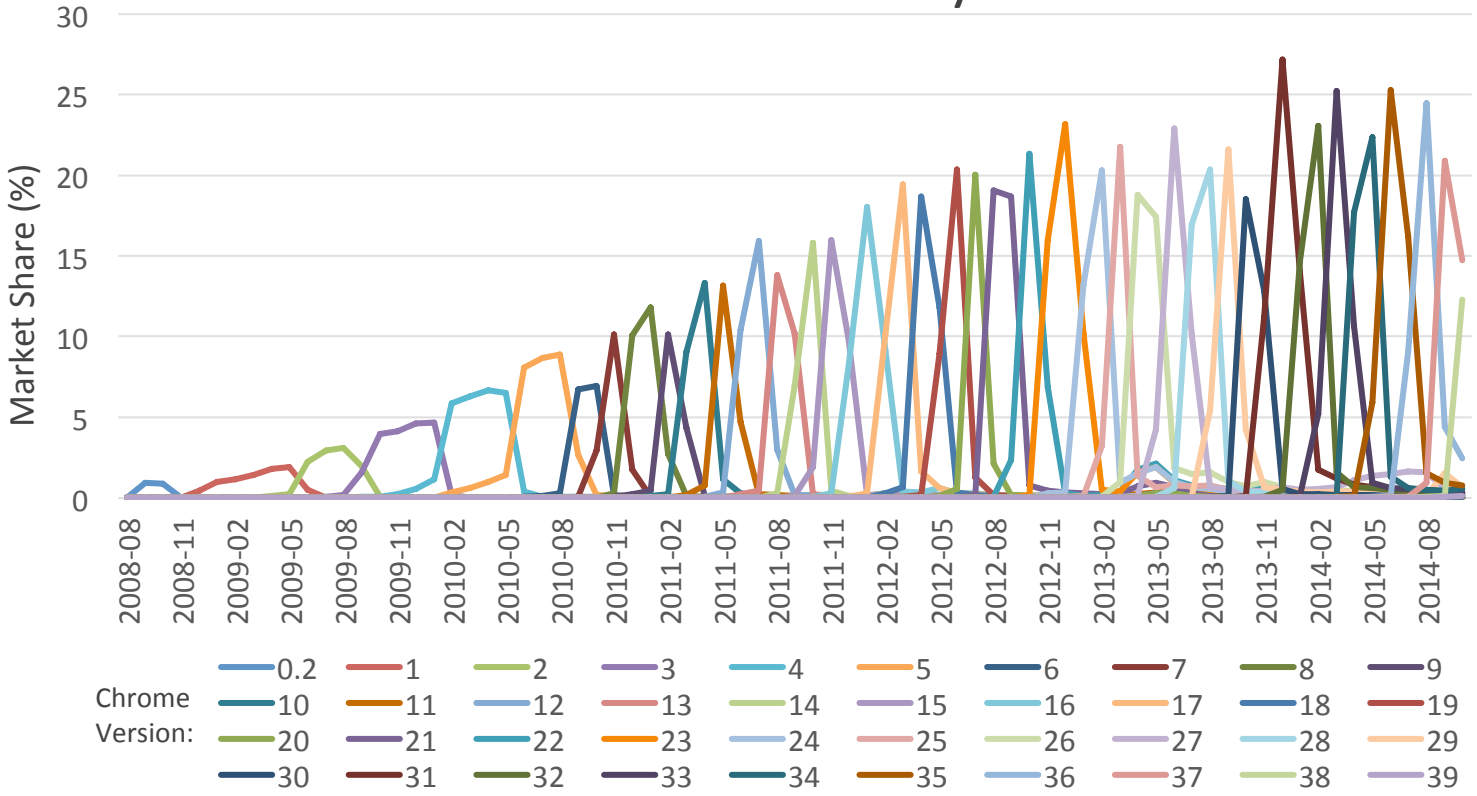
SQUID (SQLite Unknown IDentifier)

- 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



Source: StatCounter (http://gs.statcounter.com/)

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

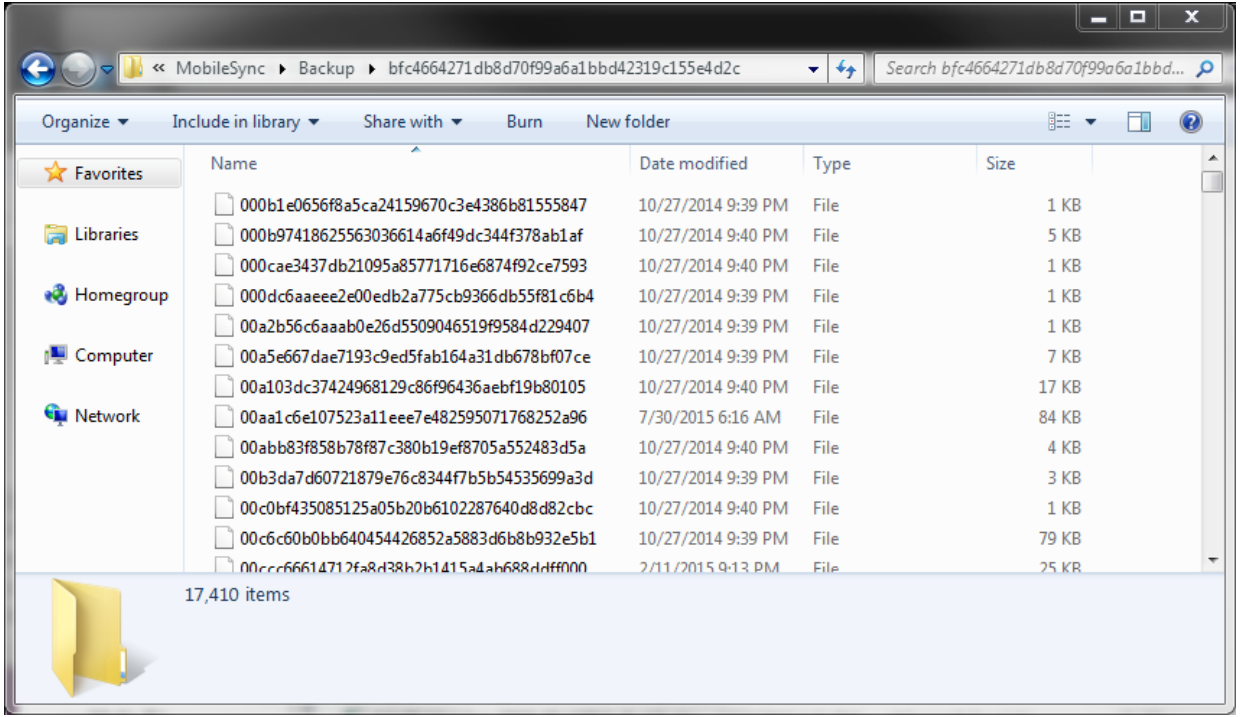
- Python script (squid.py)
- Catalog of ‘known’ databases

Comparison Commands

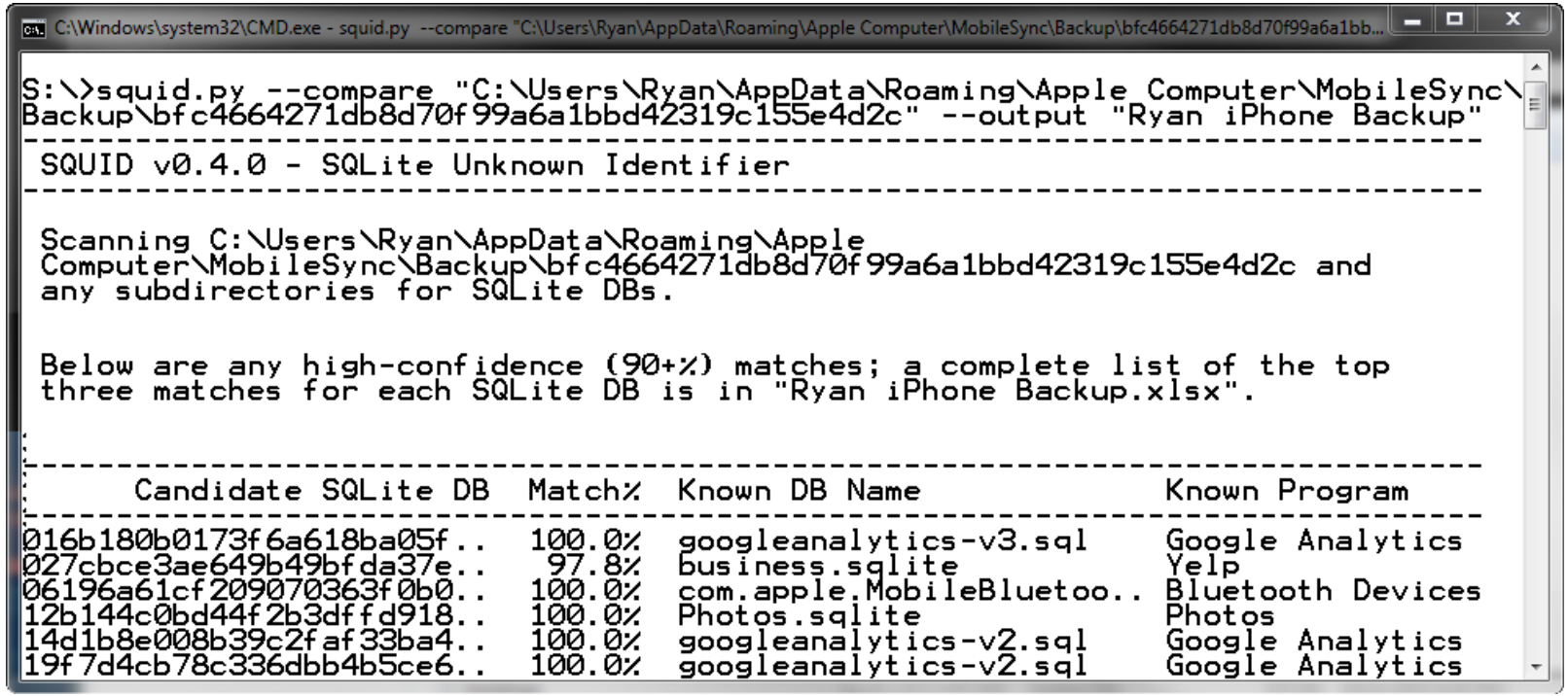
- Compare a file or directory using --compare or –c
- Name the output report (XLSX) with --output or –o

```
> squid.py --compare F:\path\to\SQLite\files
--output "E:\Reports\SQUID_Report"
```

Use Case #1: Phone Backups



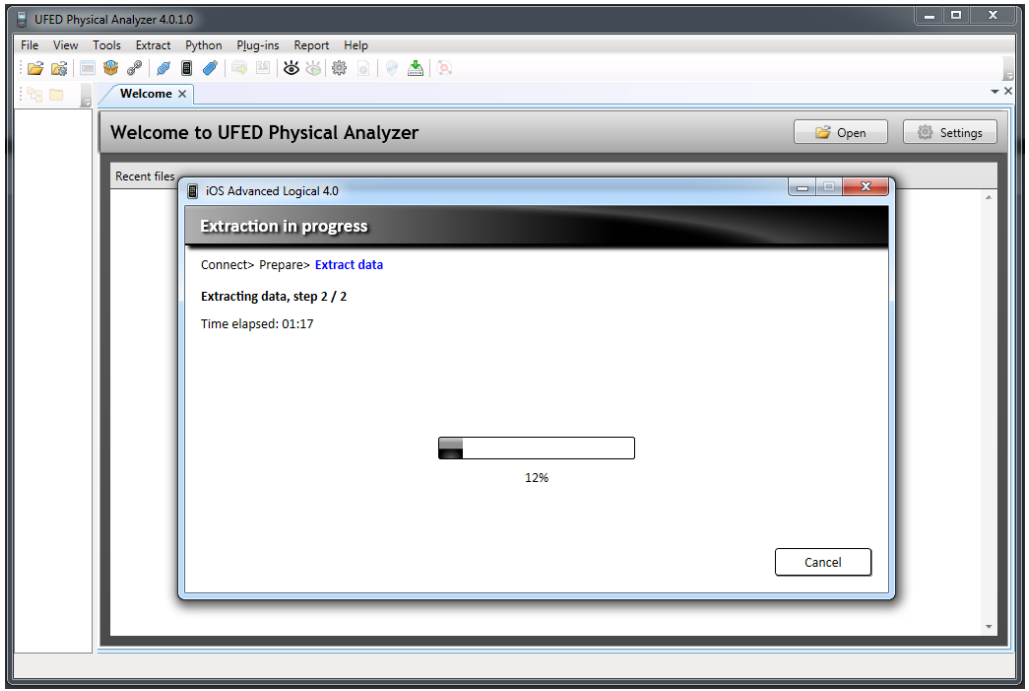
Use Case #1: Phone Backups



Use Case #1: Phone Backups

	A	B	C	D	E	F	G
1	SQUID (v0.4.0)				Match 1		
2	Name	Path	Match	DB Name	Program Name	Version	Category
60	55680ab883d0fdcffd94f959b1	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

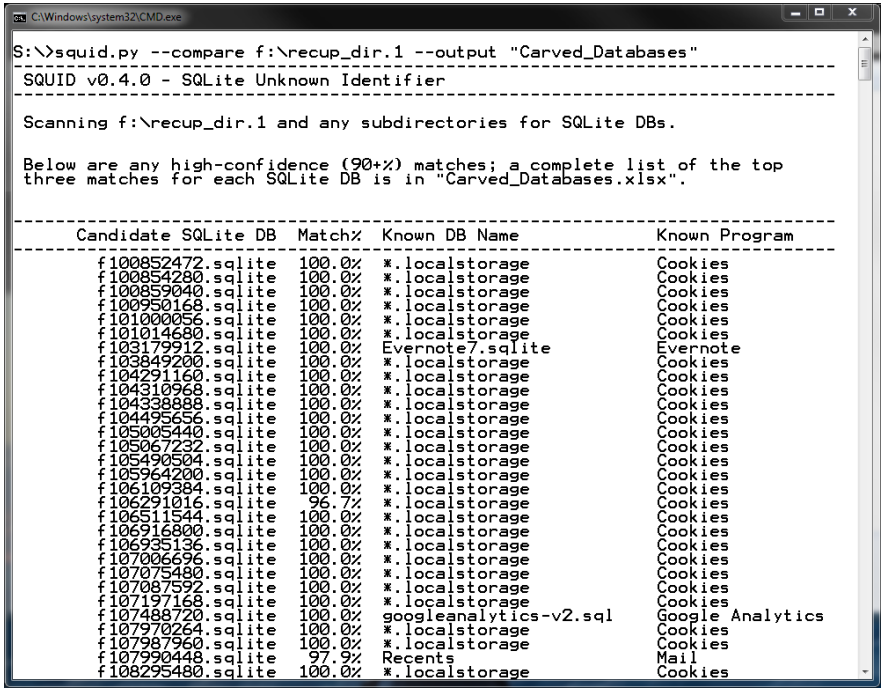


Use Case #3: Carving from Windows

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

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

- Or live file system



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