SQLite
Forensics

Il database **Free** piu' diffuso al mondo

Argomenti trattati

- Utilizzo di SQLite
  - Introduzione
  - SQL
  - Interfaccia client
- SQLite forensics
  - Carving
  - Principali applicazioni che usano SQLite
  - SQL: esempi pratici

Obiettivi

- Fornire una conoscenza di base su **SQLite** dal punto di vista architetturale e funzionale
- Presentare le principali caratteristiche dell'SQL di SQLite
- Fornire una panoramica sulle basi dati SQLite usate dai piu' comuni programmi (eg. Skype, Firefox, Chrome, ...) e di come analizzarle in ambito forensics

Argomenti non trattati

In questa presentazione non sono trattati alcuni argomenti per ragioni di spazio e di complessita'. Qualche indicazione si trova sulla pagina web http://www.xenialab.it/meo/web/index1.htm

- Internals
  - Data types
  - Strutture dati interne (file format, journal/WAL, ...)
  - Versioni ed evoluzione
- Programmazione di applicazioni
  - Interfacce di programmazione
  - Sviluppo su Android, iPhone, Windows Phone
  - Un esempio completo in C language

SQLite Introduzione

SQLite

- SQLite e' DBMS relazionale piu' installato al mondo. SQLite e' un software di pubblico dominio. I suoi principali punti di forza sono:
  - Free! Gratis e distribuito con una licenza molto, molto libera (public domain)
  - Falcilmente integrabile nelle applicazioni
  - Robustezza ed integrita' dei dati
  - Presente praticamente su ogni smartphone, su ogni MAC, sulla maggioranza dei PC, disponibile su tutti i sistemi operativi, utilizzato da centinaia di programmi, ...
  - Un ottimo e completo SQL utilizzabile direttamente e con i piu' diffusi linguaggi di programmazione

Diffusione

- SQLite e' utilizzato da:
  - Tutti i cellulari Android ed iPhone
  - Programmi diffusissimi (stima > 70% PC):
    - Firefox, Chrome, Skype, Thunderbird, Dropbox, ...
  - I piu' recenti cellulari Symbian
  - Tutti i sistemi MAC OS X e Solaris 10
  - Molti lettori MP3
  - ...

Si stima un utilizzo superiore a 500.000.000 installazioni

Architettura

L'architettura di SQLite e' semplice. Un database SQLite e' costituito da un solo file. Non c'e' nessun programma, thread o processo. Per accedere a SQLite un'applicazione deve semplicemente utilizzare la libreria disponibile come software di pubblico dominio.

Il formato del file e' definito in modo preciso dalle specifiche ed inizia con stringa: “SQLite format 3\0”. Il formato e' binary compatible su TUTTE le piattaforme.

Sono disponibili diversi programmi per accedere in modo semplice ai dati.

SQL

- SQLite supporta lo standard **ANSI SQL92** in modo praticamente completo (sono pochissimi sono i costrutti non implementati). SQLite e' semplice da utilizzare da linea di comando:

```
$ sqlite3 my.db
SELECT dept.location, count(*), sum(salary)
from emp, dept
where emp.deptno=dept.deptno
group by dept.location
order by 3 desc
limit 10;
^D
```

SQL (DDL)

- I comandi di DDL sono SQL Standard (eg. create table)
- SQLite utilizza 5 differenti Storage Class:
  - NULL, INTEGER, REAL, TEXT, BLOB
- Non c'e' un formato per le date che vengono memorizzate come testo (eg. ISO8601: YYYY-MM-DD HH:MM:SS.SSS) o come numerico (eg. secondi da Epoch)
- Sono presenti gli indici (B-tree)
- Sono presenti le viste (not updatable)
- E' disponibile una (una!) tabella di data dictionary: **sqlite_master**

SQL (DML)

- DML: Data Manipulation Language

```
sqlite> select date('now'), sqlite_version(), sqlite_source_id(),
  sqlite_compileoption_get(0), sqlite_compileoption_get(1);

 2012-02-07|3.7.6|2011-04-12 01:58:40
  f9d43fa363d54beab6f45db005abac0a7c0c47a7|ENABLE_COLUMN_METADATA|
  ENABLE_FTS3
```

```
SQLite=# select * from sqlite_master;

...
```

```
SQLite=# insert ... ; update ... ; delete ...;
```

SQL (funzioni)

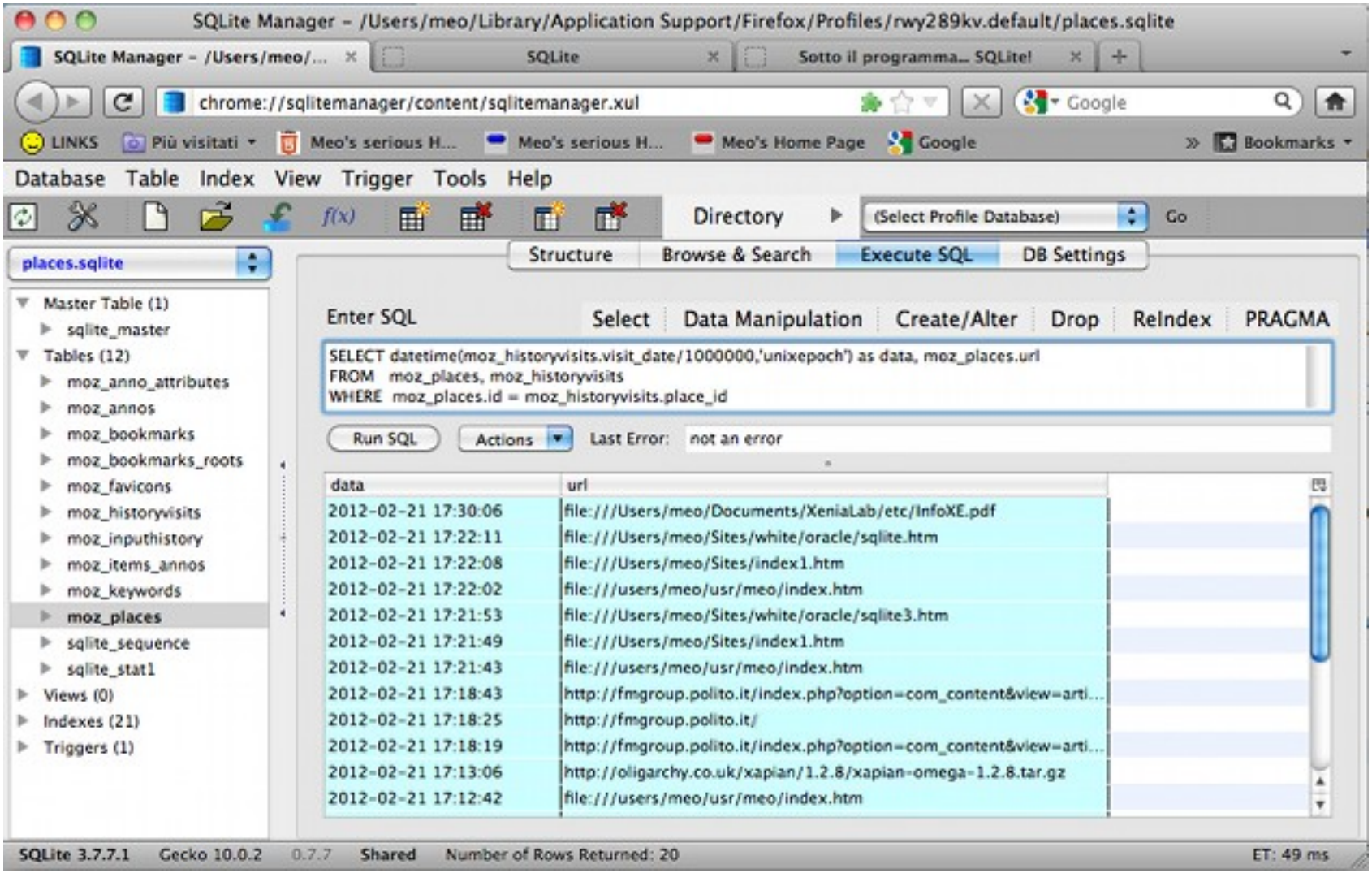
- SQLiteQL ha un insieme molto ampio di operatori, funzioni e clausole:
  - Operatori:
    AND, OR, NOT, BETWEEN ,IN, IS, =, >=, ...
  - Funzioni su stringhe, date:
    LENGTH, UPPER, LOWER, QUOTE,... RANDOM, ROUND, ... DATE, STRFTIME, ...
  - Funzioni di gruppo:
    COUNT(), SUM(), AVG(), HAVING, ...

SQLite Forensics

GUI


evidence
LXTerminal
computer forensics
network forensics
deft 7
incident response
Accessori
Audio e Video
DEFT
Grafica
Internet
Services
Ufficio
Wine
Strumenti di sistema
Preferenze
Esegui
Chiudi sessione
Analisys tools
Antimalware tools
Carving tools
Hashing tools
Imaging tools
Mobile Forensics
Network Forensics
OSINT tools
Password recovery
Reporting tools
File Manager
Gestore dischi
Midnight Commander
Mount ewf
MountManager
Wipe
Xmount
Bbwhatsapp
BitPim
Ipddump
Iphone Analyzer
iPhone backup analyzer
SQLite database browser
01:07

GUI


SQLite Manager - /Users/meo/Library/Application Support/Firefox/Profiles/rwy289kv.default/places.sqlite
chrome://sqlitemanager/content/sqlitemanager.xul
Database Table Index View Trigger Tools Help
Directory
(Select Profile Database)
Go
places.sqlite
Structure Browse & Search Execute SQL DB Settings
Master Table (1)
sqlite_master
Tables (12)
moz_anno_attributes
moz_annos
moz_bookmarks
moz_bookmarks_roots
moz_favicons
moz_historyvisits
moz_inputhistory
moz_items_annos
moz_keywords
moz_places
sqlite_sequence
sqlite_stat1
Views (0)
Indexes (21)
Triggers (1)
Enter SQL
Select Data Manipulation Create/Alter Drop ReIndex PRAGMA
SELECT datetime(moz_historyvisits.visit_date/1000000,'unixepoch') as data, moz_places.url
FROM moz_places, moz_historyvisits
WHERE moz_places.id = moz_historyvisits.place_id
Run SQL
Actions
Last Error: not an error
data
url
2012-02-21 17:30:06 file:///Users/meo/Documents/XeniaLab/etc/InfoXE.pdf
2012-02-21 17:22:11 file:///Users/meo/Sites/white/oracle/sqlite.htm
2012-02-21 17:22:08 file:///Users/meo/Sites/index1.htm
2012-02-21 17:22:02 file:///users/meo/usr/meo/index.htm
2012-02-21 17:21:53 file:///Users/meo/Sites/white/oracle/sqlite3.htm
2012-02-21 17:21:49 file:///Users/meo/Sites/index1.htm
2012-02-21 17:21:43 file:///users/meo/usr/meo/index.htm
2012-02-21 17:18:43 http://fmgroup.polito.it/index.php?option=com_content&view=arti...
2012-02-21 17:18:25 http://fmgroup.polito.it/
2012-02-21 17:18:19 http://fmgroup.polito.it/index.php?option=com_content&view=arti...
2012-02-21 17:13:06 http://oligarchy.co.uk/xapian/1.2.8/xapian-omega-1.2.8.tar.gz
2012-02-21 17:12:42 file:///users/meo/usr/meo/index.htm
SQLite 3.7.7.1 Gecko 10.0.2 0.7.7 Shared Number of Rows Returned: 20 ET: 49 ms

scalpel.conf

Il carving di un DB SQLite e' molto semplice!
I primi 16 byte contengono la scritta:
SQLite format 3\0

```
#-------------------------------------------------------------------
# SQLITE DATABASE FILES
#-------------------------------------------------------------------
#
# SQLite
     sqlitedb y 20000000000 \x53\x51\x4C\x69\x74\x65\x20\x66\x6F\x72\x6D\x61\x74\x20\x33
#
#
#
```

SQLite nei programmi

Firefox

Firefox utilizza una dozzina di database SQLite. Il piu' interessante e' il database **places.sqlite** che contiene una dozzina di tabelle tra cui il log delle URL visitate

Su Windows XP: C:\Documents and Settings\%user\Application Data\Mozilla\Firefox\Profiles\%profile.default\ - Windows Vista: C:\Users\%user\AppData\Roaming\Mozilla\Firefox\Profiles\ %profile.default\

Firefox

Ultimi siti visitati con Firefox

```
SELECT datetime(moz_historyvisits.visit_date/1000000,'unixepoch') as data,
moz_places.url
FROM   moz_places, moz_historyvisits
WHERE  moz_places.id = moz_historyvisits.place_id
ORDER BY 1 desc
LIMIT 20 OFFSET 0
```

Siti piu' visitati con Firefox

```
SELECT moz_places.url, visit_count
FROM   moz_places
ORDER BY visit_count desc
LIMIT 20
```

Chrome

Chrome utilizza diversi database SQLite tra cui il piu' significativo e' **History** che contiene gli accessi alle pagine web. Le tabelle piu' interessanti sono **ulrs**, **visits** e **downloads**.

Su Windows XP: C:\Documents and Settings\%user\Application Data\Google\Chrome\default\ - Windows Vista: C:\Users\ %user\AppData\Local\Google\Chrome\default\ ...

Chrome

Siti visitati con Chrome

```
SELECT datetime((visit_time-11644473600000000)/1000000,'unixepoch', 'localtime')
as data,
      urls.url, urls.title as titolo
FROM  urls, visits
WHERE urls.id = visits.url
ORDER BY 1 desc
LIMIT 20 OFFSET 0
```

Safari

Safari e' il diffuso browser sviluppato Apple. Il file di database e' **Cache.db** e contiene 5 tabelle.

Su Mac OS X: /Users/%user/Library/Caches/com.apple.Safari.

Safari

Siti visitati con Safari

```
SELECT cfurl_cache_response.time_stamp as data,
       cfurl_cache_response.request_key as url
FROM   cfurl_cache_response
ORDER BY 1 desc
LIMIT 20 OFFSET 0
```

Pagine richieste con Safari

```
SELECT  cfurl_cache_response.time_stamp as data,
        cfurl_cache_response.request_key as url,
        cfurl_cache_blob_data.receiver_data as contenuto
FROM    cfurl_cache_blob_data, cfurl_cache_response
WHERE   cfurl_cache_blob_data.entry_ID=cfurl_cache_response.entry_ID
ORDER BY 1 desc
LIMIT 20 OFFSET 0
```

Skype

Skype mantiene i propri dati sul database file **main.db** che contiene una decina di tabelle.

Su MS Windows il database di Skype si trova in C:\Documents and Settings\%profile\Application Data\Skype\%skype_user, con l'eccezione di Vista and 2008 dove il file e' in C:\Documents and Settings\%profile\AppData\Roaming\Skype\%skype_user. Su Mac OS X: /Users/%user/Library/Application Support/Skype/%skype_user.

Skype

Chiamate skype-to-phone (tutte) e skype-to-skype (solo se OK)

```
SELECT identity as chiamante, guid, call_duration/60 as durata_minuti,
          strftime('%Y-%m-%d %H:%M:%S', start_timestamp,'unixepoch','localtime')
               as inizio_chiamata
FROM   CallMembers
ORDER BY id
```

Chiamate skype-to-skype (tutte)

```
SELECT host_identity as chiamante, current_video_audience as destinazione,
          duration/60 as durata_minuti,
          strftime('%Y-%m-%d %H:%M:%S', begin_timestamp,'unixepoch','localtime')
               as inizio_chiamata
FROM   Calls
ORDER BY id
```

Skype

Chat Skype

```
SELECT author as chiamante, chatname, body_xml as messaggio,
       strftime('%Y-%m-%d %H:%M:%S', timestamp,'unixepoch','localtime') as
inizio_chiamata
FROM   messages
ORDER BY timestamp
```

Apple iPhone

I sistemi operativi della Apple utilizzano in modo estensivo il database SQLite. iOS, il sistema operativo dell' **iPhone** non fa eccezione.

Tra i molti DB interessanti: sms.db, consolidated.db (iOS >= 4), ...

Sul DB consolidated.db vi sono state polemiche ed e' stata emessa un patch specifica per rimuovere parte dei dati storici, ma l'informazione era gia' presente da tempo!

Apple iPhone

SMS

```
SELECT ROWID, case flags when 2 then 'Ricevuto' when 3 then 'Inviato'
                    when 33 then 'Fail'  when 129 then '*Del' else 'Unkn' end as tipo,
      address as numero_tel, datetime(date,'unixepoch','localtime') as data,
      text as messaggio
FROM   message
```

Dove sei stato?

```
SELECT datetime(Timestamp+978307200,'unixepoch','localtime') as Time,
      Latitude, Longitude, 'WiFi' as Source
FROM   WifiLocation
UNION
SELECT datetime(Timestamp+978307200,'unixepoch','localtime') as Time,
      Latitude, Longitude, 'Cell' as Source
FROM   CellLocation
ORDER BY 1;
```

Android

Android utilizza SQLite su molteplici applicazioni.

Ad esempio: contacts.db accounts.db im.db media.db mms.db sms.db telephony.db settings.db maps.db ...

Android

SMS

```
SELECT datetime(date/1000,'unixepoch','localtime') as data, address as indirizzo,
subject as soggetto, body as testo
FROM   sms
ORDER BY date desc
```

Statistica chiamate

```
SELECT number as numero, number_key as chiave,
      count(*) as numero, sum(duration) as durata,
      min(datetime(date/1000,'unixepoch','localtime')) as prima_chiamata,
      max(datetime(date/1000,'unixepoch','localtime')) as ultima_chiamata
FROM   calls
GROUP BY number, number_key
ORDER BY 3 DESC
LIMIT 20
```

Qualcosa in piu'...

Agendo direttamente in SQL possono essere evidenziate in modo molto semplice tutte le cancellazioni logiche (eg. iPhone SMS).

I dispositivi Mobile usano una versione di SQLite compilata senza l'autovacuum ==> e' possibile recuperare anche i dati cancellati analizzando la struttura binaria del file di database.

Vi sono alcuni programmi (a pagamento) che consentono l'analisi dei record cancellati. In ogni caso la struttura di un database SQLite e' completamente documentata ed e' relativamente semplice da analizzare in binario con un hexdump o simili...

Varie ed eventuali

- Domande e risposte

- Link utili

http://www.SQLite.org/

Sito ufficiale SQLite

http://www.xenialab.it/meo/web/index1.htm

Non ufficiale ma c'e' molta documentazione... in italiano!

by meo bogliolo