Preiskovanje spletnih brskalnikov v operacijskem sistemu Linux

1. Preiskovanje spletnega brskalnika Firefox

Spletni brskalnik Firefox shranjuje podatke o uporabnikovem brskanju v datoteke tipa *sqlite*. SQLite je datoteka narejena v programskem jeziku C, ki vsebuje relacijske podatkovne baze. Brskalnik Firefox shranjuje sqlite datoteke z informacijami o uporabniškem brskanju v mapi:

`~/.mozilla/firefox/<PROFILE>/`

Med drugimi imamo v mapi naslednje datoteke:

- addons.sqlite – podatki o nameščenih dodatkih,
- cookies.sqlite – podatki o shranjenih piškotih,
- downloads.sqlite – podatki o snetih datotekah, ki se še nahajajo v oknu Prenosi,
- extensions.sqlite – podatki o razširitvah,
- formhistory.sqlite – podatki o uporab. vnešenih podatkih v vnosna polja v obrazcih,
- places.sqlite – podatki o zgodovini brskanja,
- search.sqlite – podatki o iskalnih nizih,
- ter ostale.

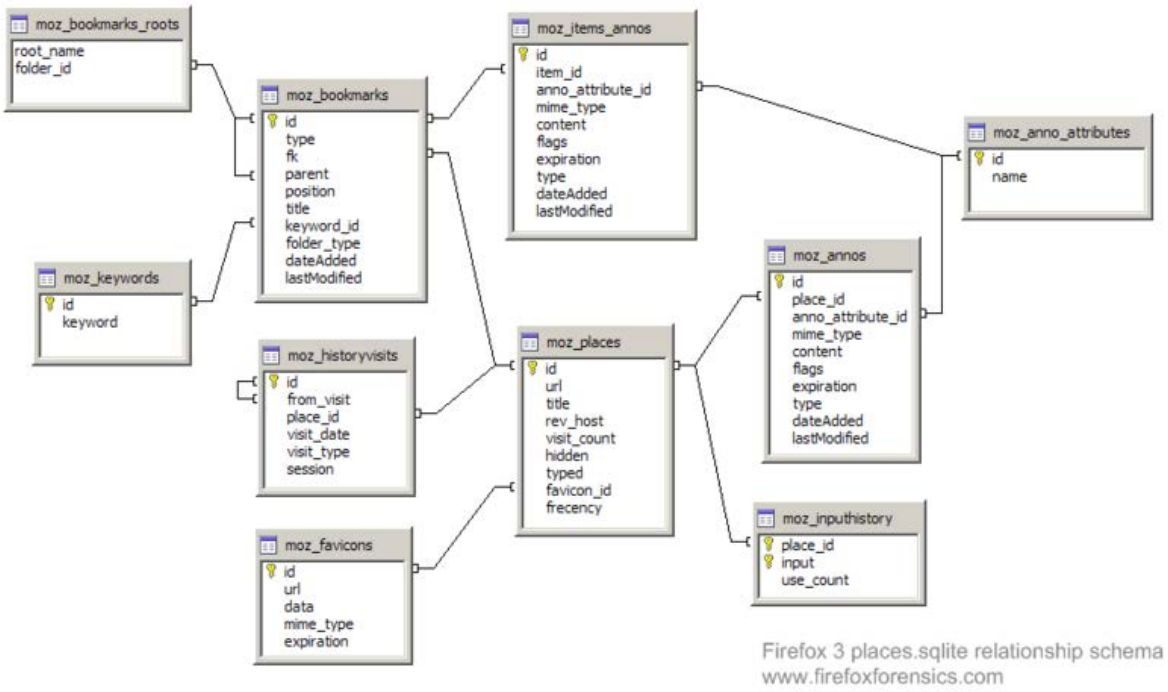
Datoteka *Cookies.sqlite* vsebuje tabelo *moz_cookies*, ki pa je sestavljena naslednji shemi.

moz_cookies [id; name; value; host; path; expiry; lastAccessed; isSecure; isHttpOnly; baseDomain; creationTime]

Datoteka *Formhistory.sqlite* vsebuje tabelo *moz_formhistory*.

moz_formhistory [id; fieldname; value; timesUsed; firstUsed; lastUsed; guid]

Relacijska shema podatkovne baze znotraj datoteke *places.sqlite* je bolj kompliciran in je prikazana na sliki 1, v njej pa so shranjeni podrobni podatki o zgodovini brskanja uporabnika.



Slika : Relacijska shema znotraj places.sqlite

Časovni žigi znotraj podatkovnih tabel so tipa *PRTime*. Gre za število mikrosekund od 1.1.1970 dalje, zapisanih v 64-bitnem številskem tipu. Stolpec *visit_type* označuje tip prehoda na spletno stran (ali je uporabnik vpisal naslov spletne strani v url okence, ali je bil preusmerjen preko povezave ipd.).

Vsebino *sqlite* datotek je možno prebirati s pomočjo orodja SQLite. S pomočjo spodnjega ukaza, lahko uporabnik na svoj operacijski sistem namesti orodje sqlite3, ki je le eden od orodij za pregledovanje sqlite datotek.

```
apt-get install sqlite3
```

Uporabnik lahko, za preiskovanje sqlite datotek, namesti in uporablja tudi orodja z grafičnim vmesnikom. Nekatera znana orodja so *SQLiteMan* ali *SQLiteBrowser*. Prav tako je mogoče namestiti *SQLite Manager*, dodatek za spletni brskalnik Firefox. Po namestitvi lahko orodje odpremo preko brskalnika Firefox (Tools -> SQLite Manager).

Preiskovalec za preiskovanje sqlite datoteke lahko uporablja *sqlite3* ali katerega od ostalih SQLite brskalnikov. Za analizo tabel najprej poženemo orodje sqlite3 na način, da v terminalu vpišemo `sqlite3 <ime_datoteke.sqlite>`.

Po zagonu sqlite preidemo v program. S pomočjo ukaza

```
sqlite>.tables
```

vidimo vse podatkovne tabele shranjene znotraj datoteke. Z ukazom

```
sqlite>.schema <ime_tabele>
```

vidimo shemo podatkovne tabele. Ostale možnosti uporabe sqlite orodja vidite s pomočjo ukaza `.help`.

Za preiskovanje tabel uporabljamo *strukturirani povpraševalni jezik SQL*.

Spodnji primer prikazuje pridobivanje zgodovine brskanja skupaj z url naslovom, naslovom strani in časom, pretvorjenim v ljudem bolj berljiv zapis.

```
sqlite>SELECT datetime(moz_historyvisits.visit_date/1000000,
'unixepoch') as date, moz_places.url
 ...>FROM moz_places, moz_historyvisits
 ...>WHERE moz_places.id = moz_historyvisits.place_id
 ...>ORDER BY date DESC;
```

Spodnji primer prikazuje vse obiskane strani v nekem časovnem okviru:

```
sqlite>SELECT datetime((visit_date/1000000), 'unixepoch',
'localtime') as date, p.url, p.title
 ...>FROM moz_places p, moz_historyvisits
 ...>WHERE date BETWEEN '2012-04-02 00:00:00' AND '2012-04-04
00:00:00'
 ...>ORDER BY date DESC;
```

2. Preiskovanje spletnega brskalnika Google Chrome

Na operacijske sistemu Linux lahko uporabnik uporablja *Google Chrome* ali *chromium-browser*. Google Chrome temelji na odprtokodnem projektu Chromium. Brskalnika se v manjši meri ločita med sabo, pomembno je vedeti, da uporabljata različne mape za shranjevanje uporabniškega profila.

Spletni brskalnik Chromium shranjuje svojo zgodovino brskanja v mapo chromium znotraj:

```
~/.config/chromium/
```

Medtem, ko Google Chrome za shranjevanje uporablja mapo google-chrome:

```
~/.config/google-chrome/
```

Zgodovino in ostale informacije prav tako shranjujeta v sqlite datoteko (kljub temu, da datoteke nimajo .sqlite končnice), ki jo lahko analiziramo na podoben način, kot pri brskalniku Firefox.

Znotraj mape google-chrome se nahajajo med drugimi tudi naslednje datoteke:

- Favicons – informacije o ikonah spletnih strani,
- History – informacije o zgodovini brskanja,

- Bookmarks – informacije o zaznamkih,
- Archived History – informacije o arhivirani zgodovini,
- Top Sites,
- Cookies – informacije o piškotkih,
- in še mnogo ostalih. Uporabnik lahko pregleda mapo z ukazom *ls -al*.

Struktura tabel znotraj datoteke *History* je sledeča:

- downloads – vsebuje seznam pobranih datotek.
- presentation
- urls – vsebuje podatke o obiskanih spletnih straneh.
- keyword_search_terms
- segment_usage
- visits – vsebuje informacije o obiskih (časovni žigi, ...)
- meta – vsebuje metapodatke
- segments

Uporabnik za preiskovanje sqlite datoteke lahko uporablja sqlite3 ali katerega od ostalih SQLite brskalnikov. Za analizo tabel najprej poženemo orodje sqlite3 na način, da v terminalu vpišemo `sqlite3 <ime_datoteke>`. V kolikor je ime datoteke ločeno s presledkom, moramo ime datoteke navesti v narekovaje, primer: `sqlite3 "Top Sites"`.

Pomembno je omeniti, da časovni žigi znotraj tabel niso povsod v epoch zapisu (primer tabela *visits*). V takšnih primerih so časovni žigi zapisani v mikrosekundah od 1.1.1601 dalje. Nekatere tabele imajo časovne žige v PRTime zapisu, število sekund od 1.1.1970 (primer downloads).

Znotraj tabele *visits* se nahaj stolpec transition, ki opisuje način, kako je uporabnik prišel na stran, podobno kot je to opisano pri brskalniku Firefox. Obstaja 11 t.i. prehodnih tipov med stranmi. 0 – pomeni, da je uporabnik prišel na stran preko povezave, 1 – uporabnik je vpisal url povezavo v brskalnik, potem sledijo še začetna stran, oddaja obrazcev, osvežitev strani itd.

Spodnji primer prikazuje pridobivanje podatkov o zgodovini brskanja (url naslov in naslov strani), prav tako opravimo pretvorbo časovnega žiga v ljudem bolj berljiv format.

```
sqlite>SELECT datetime(((visits.visit_time/1000000)-11644473600),
"unixepoch") as time, urls.url, urls.title
 ...>FROM urls, visits
 ...>WHERE urls.id = visits.url
 ...>ORDER BY time;
```

Časovnemu žigu odštejemo število sekund od 1.1.1601 do 1.1.1970.
S pomočjo `LIMIT <št.prikazanih vrstic>` lahko omejimo rezultat na zadnjih nekaj zapisov iz tabele.

Omenimo lahko še program *log2timeline*, ki iz datotek zgodovine brskanja zgradi sosledje dogodkov za lažje razumevanje uporabnikovega brskanja.

3. ZAKLJUČEK

Kot vidimo mora preiskovalec poleg poznavanja v kakšni obliki brskalnik shranjuje svojo zgodovino in kje jo shranjuje, poznati tudi jezik SQL, s katerim si lahko pomaga pri pridobivanju podatkov iz datotek. Seveda so za lažjo uporabo na spletu tudi grafična orodja za manipulacijo sqlite tabel, vendar bo vsaj splošno znanje SQL jezika preiskovalcu veliko v pomoč.

Pomembno je tudi omeniti, da imajo brskalniki možnost vklopa prikritega/privatnega (InPrivate) načina brskanja s katerim naj ne bi beležili zgodovine brskanja in ostalih podatkov v sqlite datoteke. Gre za način brskanja, ki ne shranjuje zgodovine oz. informacij v datoteke, če pa že, pa jih ob izhodu iz zasebnega načina ali zaprtju brskalnika, izbriše. Tak primer so piškotki, ki se izbrišejo ob zaprtju brskalnika. Vendar pa gre bolj za lokalno prikritost informacij, kajti podatki, ki se zapisujejo v registre in t.i. 'cache data', so nedotaknjeni, preko katerih forenziki še zmeraj lahko odkrijejo indice.

4. Viri in reference:

1. Eoghan Casey. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. Third Edition. Maryland, USA: Elsevier
2. Mozilla Firefox 3 History File Format. (maj 2012). Povezava: http://www.forensicswiki.org/wiki/Mozilla_Firefox_3_History_File_Format
3. Google Chrome Forensics. (maj 2012). Povezava: http://computer-forensics.sans.org/blog/2010/01/21/google-chrome-forensics/
4. Log2timeline. (maj 2012). Povezava: http://log2timeline.net/