ENGENSEC
Educating the Next generation experts in Cyber Security

Tempus

The project has been funded by the European Commission. The Education, Audiovisual and Culture Executive program (EACEA), TEMPUS IV. The content of this presentation reflects the opinion of the author.

Internet Artefacts

Digital Forensic

Developers:
C. Yesil

Browser Artifacts

- Which kinds of Browsers exists
  - Chromes
  - Firefox
  - Internet Explorer
  - Safari
  - Opera

Webbrowser functionality and artifacts

- Functions
  - Browse internet
  - Incognito / InPrivate / Private browsing
  - Sandboxing
  - Upload/download files
  - User data / Profile
  - Add-ons/extensions/plugins

- Artifacts
  - Bookmarks
  - History (browse, form, search, download)
  - Cache
  - Cookies
  - Stored credentials
  - Settings / Configuration

Browser Artifacts

- Evidence Left Behind:-
  - Cache
  - Bookmarks
  - Browsing History (visited URLs)
  - Cookies
  - Downloads
  - Stored credentials

Browser Artifacts
Internet Explorer

- Windows 7
  - C:\Users\user\AppDataLocal\Microsoft\Windows\Temporary Internet Files\
- Windows 8-10
- Extensible Storage Engine *.edb/.dat – JETBlue-Files–
- WebCacheV01.dat

Browser Artifacts
Mozilla Firefox

- %\Users\[Nutzer]\AppData\Roaming\Mozilla\Firefox\Profiles\[Profil-ID]\

- addons.sqlite
- Bookmarks.html
- places.sqlite
- cookies.sqlite
- formhistory.sqlite
- signons.sqlite

Browser Artifacts
Chrome

- %\Users\[Nutzer]\AppData\Local\Google\Chrome\User Data\default
- History
- Cookies
- Logindata .....

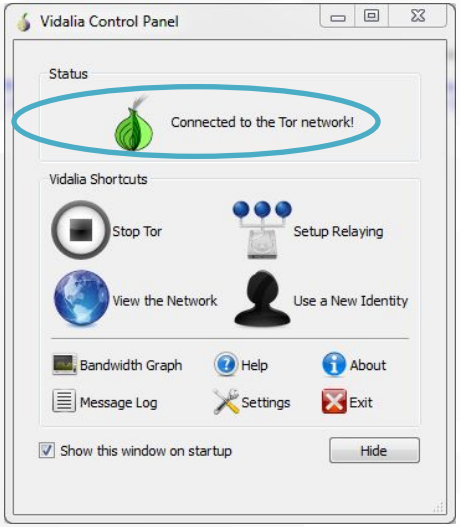
Anonymous Browsing - Tor

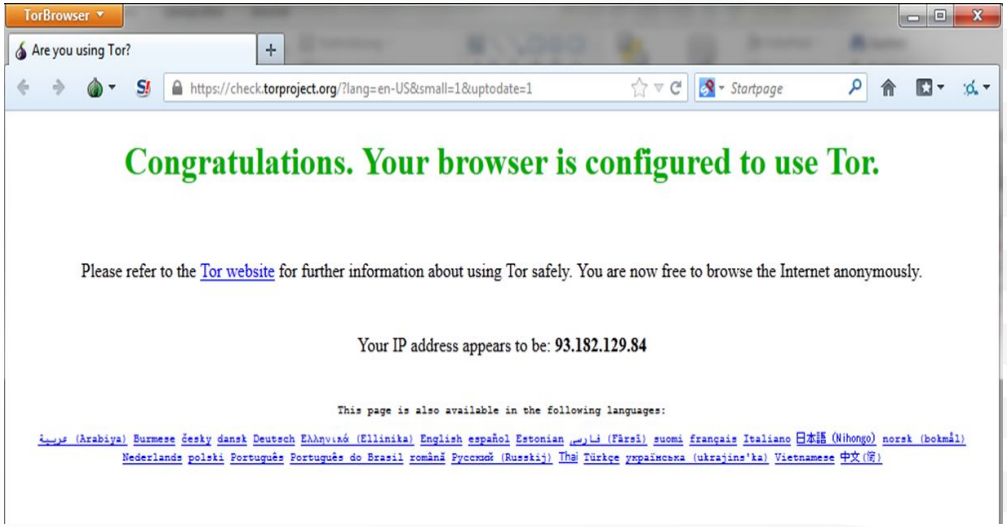
- Tor (**T**he **O**nion **R**outer)
- Portable browsers (Tor browser bundle, Portable FF)
- Use on Windows, Mac OS X, or Linux without needing to install
- Run off USB flash drive
- https://www.torproject.org
- Tor Add-On Firefox

Anonymous Browsing - Tor

- Tor Browser websites transmitted via Tor
- Runs Private Mode (website history & cookies etc. deleted)
- Only trace evidence RAM
  - RAM capture
  - RAM carving (.tor, .onion URLS)
  - Pagefile.sys (possibly)
  - Check internet history for proxies

Anonymous Browsing - Tor





New IP Address!

Anonymous Browsing - Tor

- Live operating system
- Run from DVD, USB or SD card.
- Preserves **privacy** and **anonymity**
  - Internet **anonymously** - connections go through Tor network
  - Application connecting directly to Internet - automatically **blocked**
  - Leaves **no trace** of Web Browser artifacts on the computer
- Download from https://tails.boum.org/index.en.html

Anonymous Browsing - TAILS

- Live operating system
- Run from DVD, USB or SD card.
- Preserves **privacy** and **anonymity**
  - Internet **anonymously** - connections go through Tor network
  - Application connecting directly to Internet - automatically **blocked**
  - Leaves **no trace** of Web Browser artifacts on the computer
- Download from https://tails.boum.org/index.en.html

Example Firefox Practical

- Stores information about visited Websites in SQLite Database
  - **On Win7/Vista:**

C:\Users\%USERNAME%\AppData\Roaming\Mozilla\Firefox\Profiles

\%PROFILE%.default\places.sqlite

  - **On XP:**

C:\Documents and Settings\%USERNAME%\Application Data\Mozilla\Firefox\Profiles\%PROFILE%.default\places.sqlite

  - **On Mac/OSX**

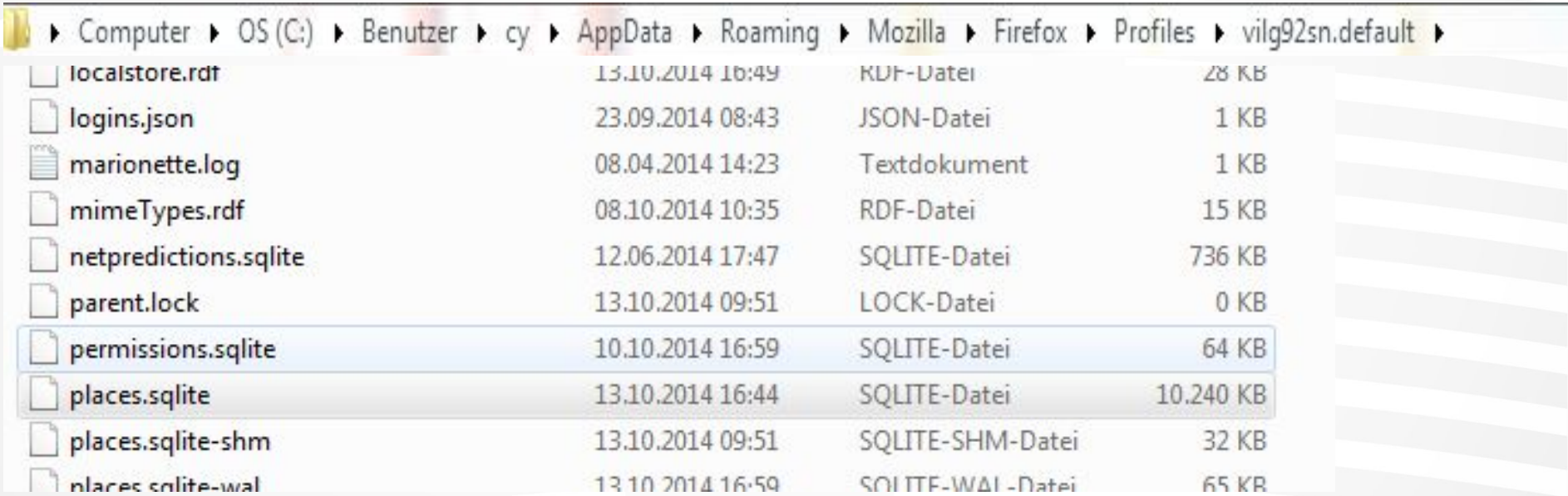
/Users/$USER/Library/Application Support/Firefox/Profiles/$PROFILE.default/places.sqlite

  - **On Linux**

/home/$USER/.mozilla/firefox/$PROFILE.default/places.sqlite

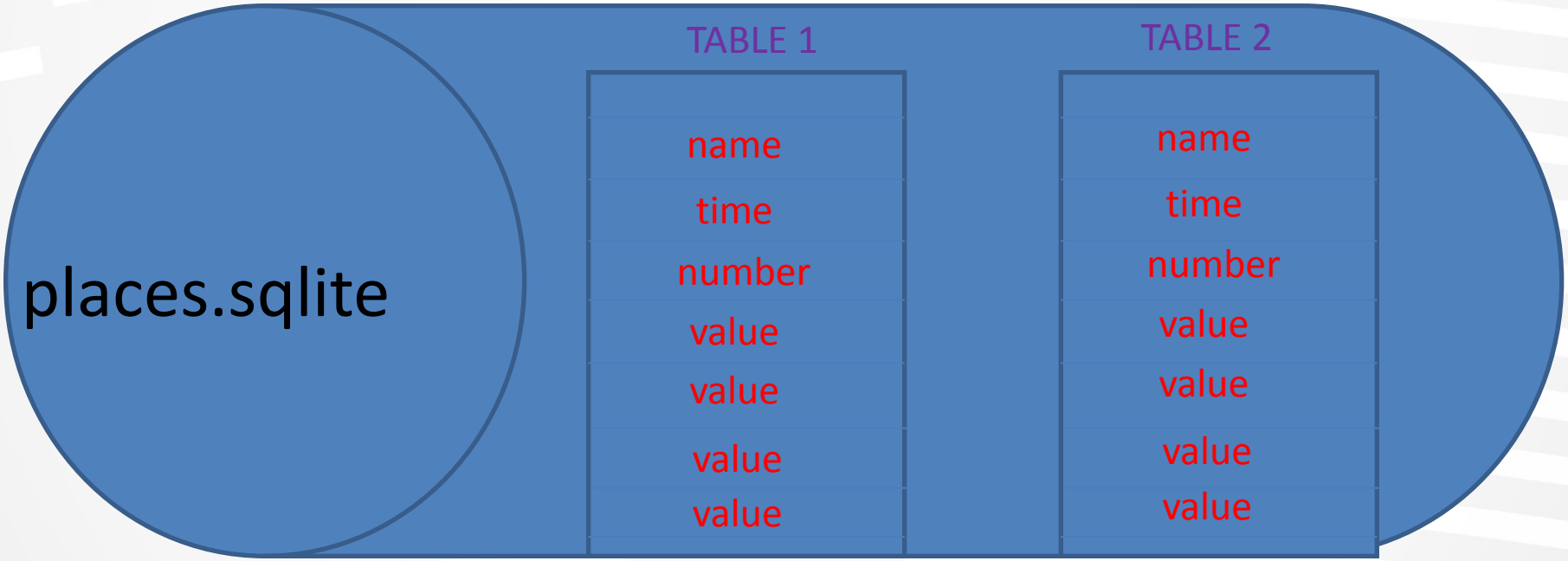
Firefox Practical

- Locate places.sqlite



Firefox Practical

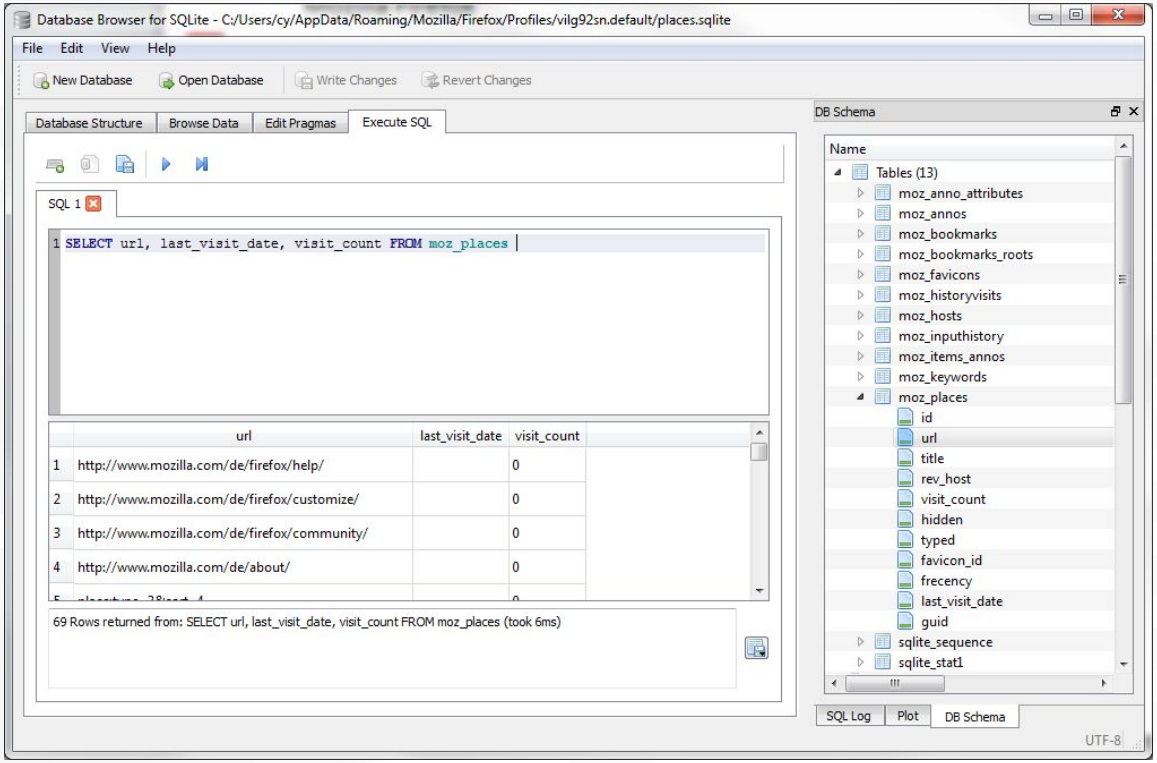
SELECT name, time, number FROM TABLE1



Firefox Practical

- **Overview of visited Websites**

SELECT url, last_visit_date, visit_count FROM moz_places

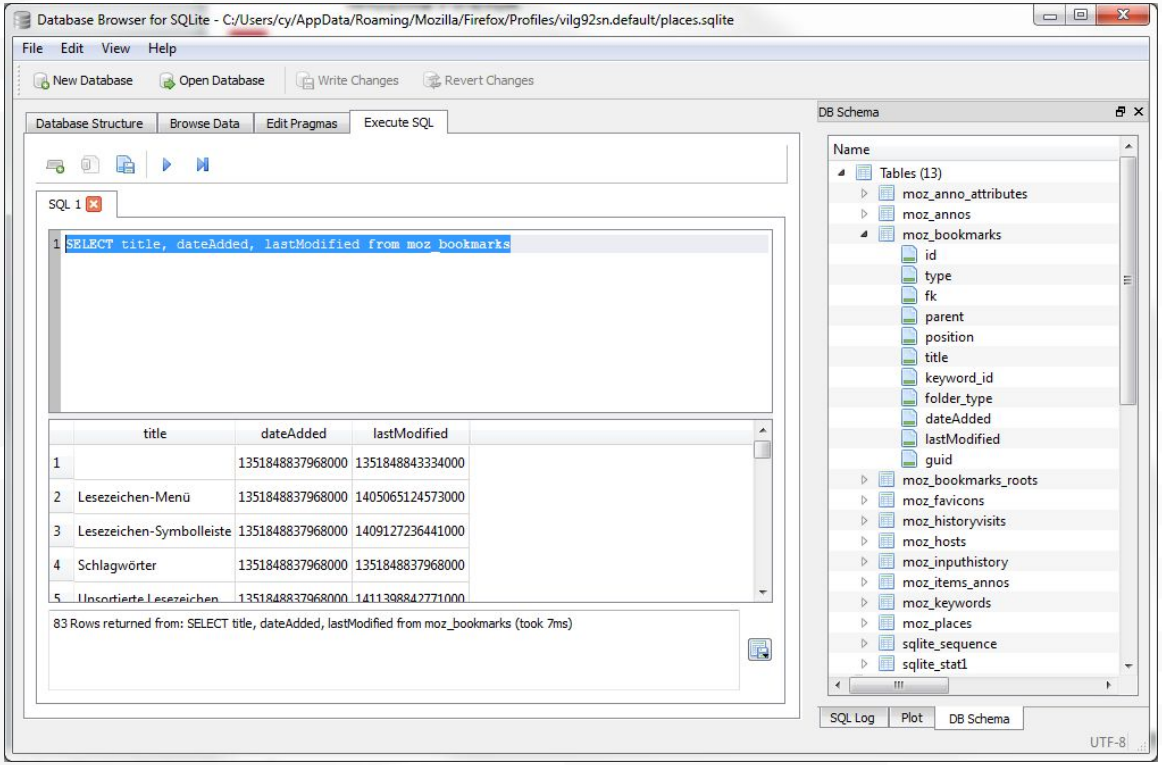


SELECT datetime(moz_places.last_visit_date/1000000, 'unixepoch', 'localtime'), url FROM moz_places

Firefox Practical

- **Bookmarks**

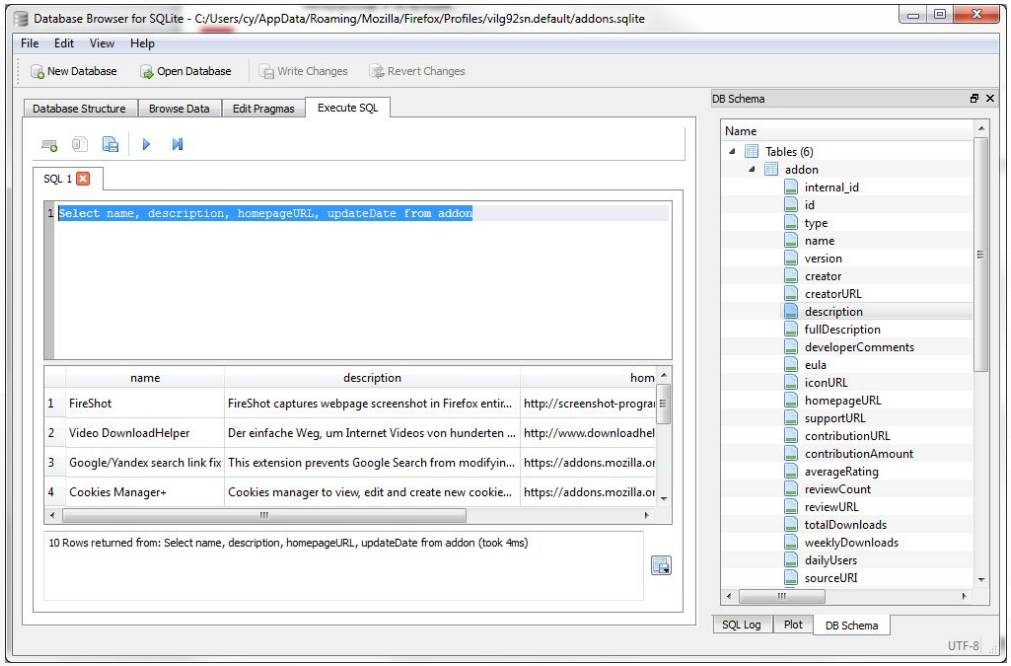
SELECT title, dateAdded, lastModified FROM moz_bookmarks



Firefox Practical

- **AddOns**

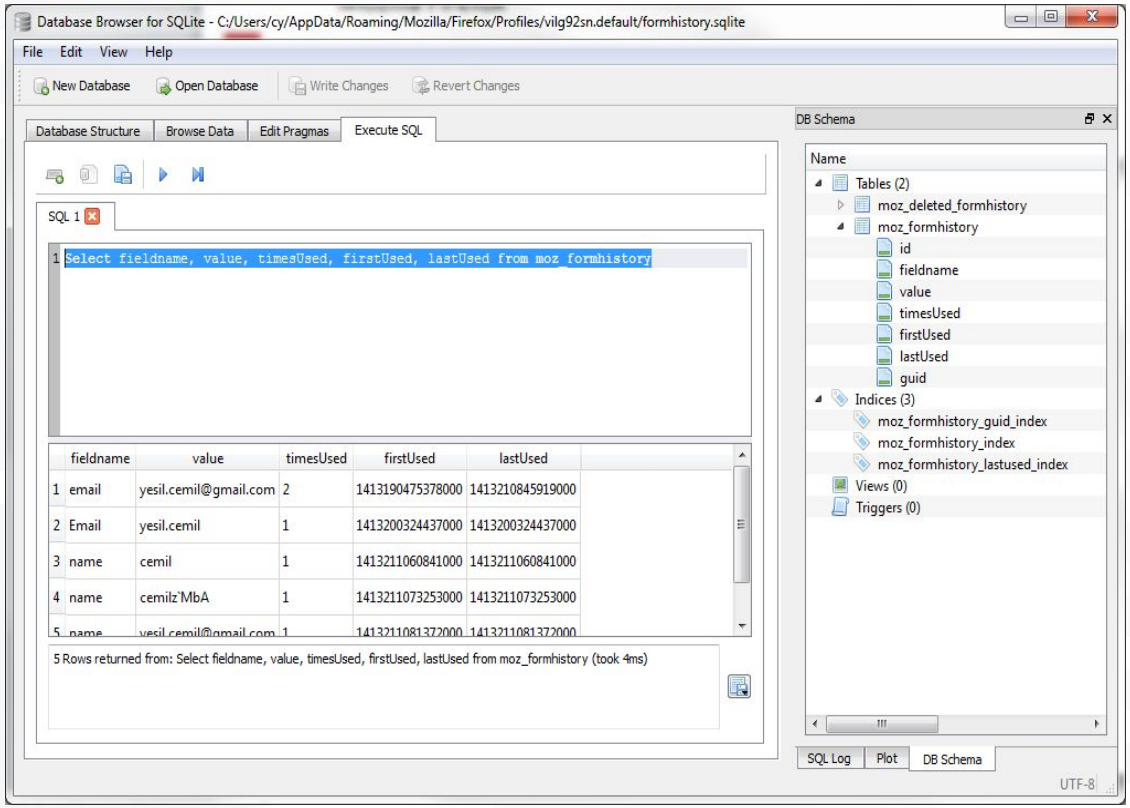
SELECT name, description, homepageURL, updateDate FROM addon



Firefox Practical

- **Form data**

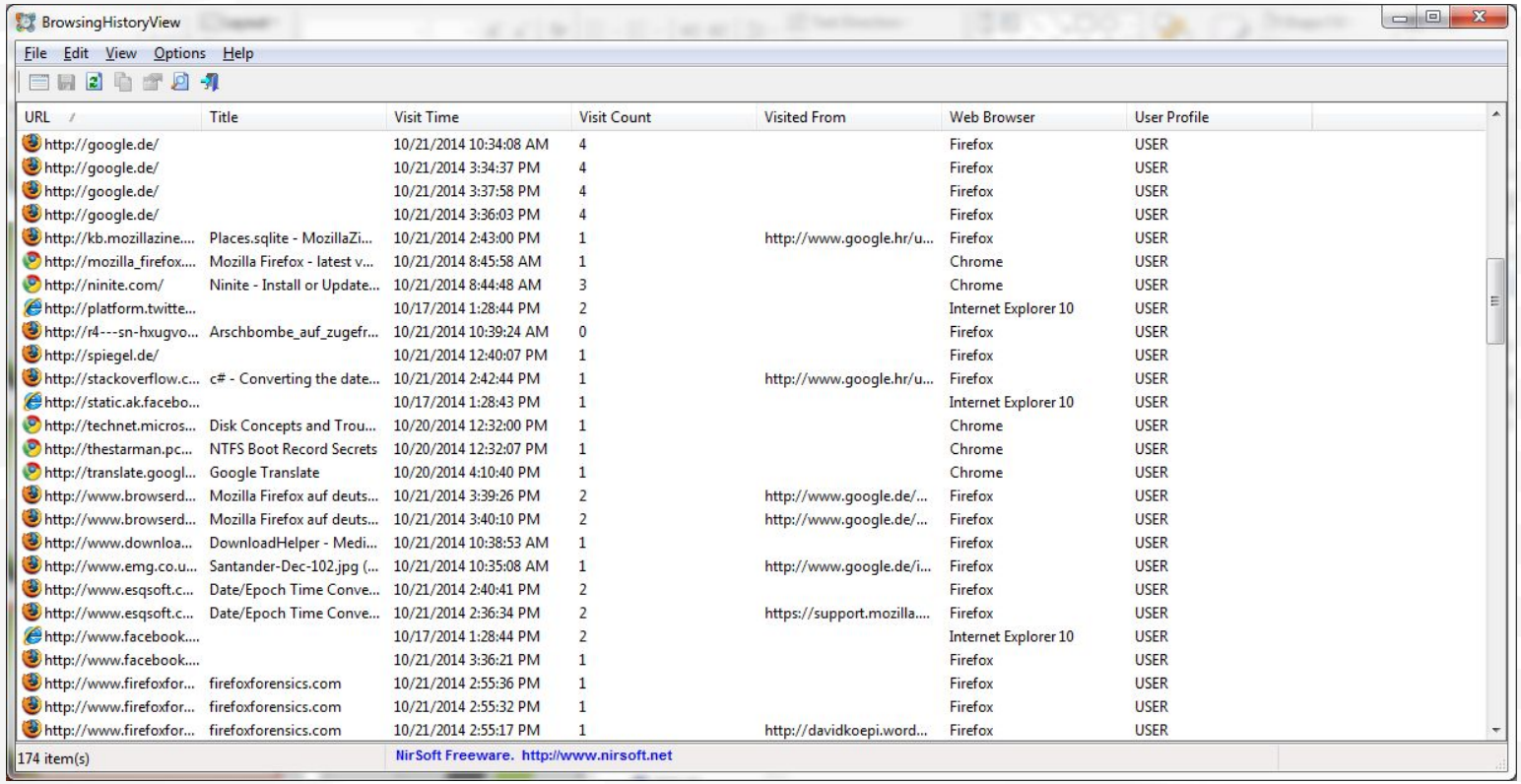
SELECT fieldname, value, timesUsed, firstUsed, lastUsed FROM moz_formhistory



Firefox Practical

Tools

- FreeTools
  - Nirsoft (http://www.nirsoft.net/utils/browsing_history_view.html)



Firefox Practical

All preferences of the User-Profile is stored in

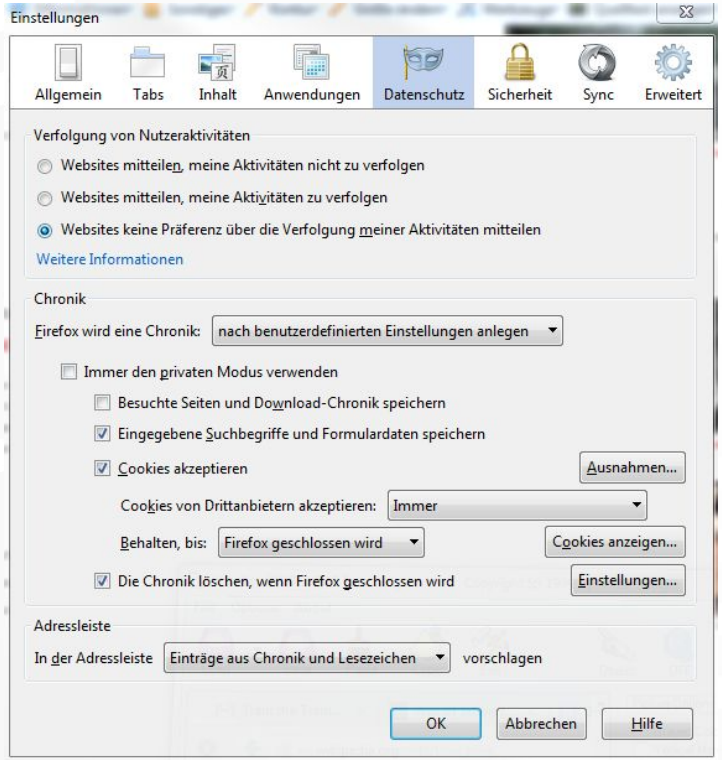
- about:config
- C:\Users\%USER%\AppData\Roaming\Mozilla\Firefox\Profiles\%Profile%\prefs.js

```
# Mozilla User Preferences

/* Do not edit this file.
 *
 * If you make changes to this file while the application is running,
 * the changes will be overwritten when the application exits.
 *
 * To make a manual change to preferences, you can visit the URL about:config
 */

user_pref("accessibility.typeaheadfind.flashBar", 0);
user_pref("app.update.lastUpdateTime.addon-background-update-timer", 1413187296);
user_pref("app.update.lastUpdateTime.background-update-timer", 1413187056);
user_pref("app.update.lastUpdateTime.blocklist-background-update-timer", 1413187416);
user_pref("app.update.lastUpdateTime.browser-cleanup-thumbnails", 1413212016);
user_pref("app.update.lastUpdateTime.experiments-update-timer", 1413187176);
user_pref("app.update.lastUpdateTime.search-engine-update-timer", 1413208536);
user_pref("app.update.migrated.updateDir", true);
user_pref("browser.bookmarks.restore_default_bookmarks", false);
user_pref("browser.cache.disk.capacity", 358400);
user_pref("browser.cache.disk.smart_size.first_run", false);
user_pref("browser.cache.disk.smart_size.use_old_max", false);
user_pref("browser.cache.disk.smart_size_cached_value", 358400);
user_pref("browser.cache.frecency_experiment", 2);
user_pref("browser.customizemode.tip0.shown", true);
user_pref("browser.download.dir", "G:\\Downloads");
user_pref("browser.download.folderList", 2);
user_pref("browser.download.importedFromSqlite", true);
user_pref("browser.download.lastDir", "C:\\Users\\cx\\Desktop\\Hacker");
user_pref("browser.download.manager.alertOnEXEOpen", true);
user_pref("browser.download.panel.firstSessionCompleted", true);
```

Privatemode
No history is stored



Oportunities:

Crash Report
RAM-Dump