

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

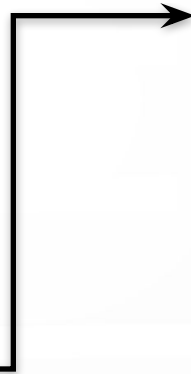
- Which kinds of Browsers exists
 - Chromes
 - Firefox
 - Internet Explorer
 - Safari
 - Opera



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



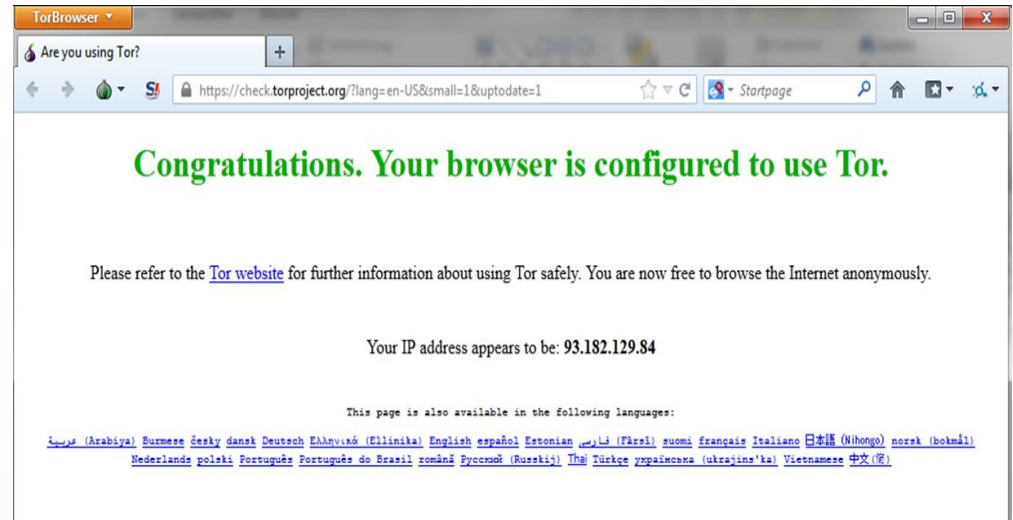
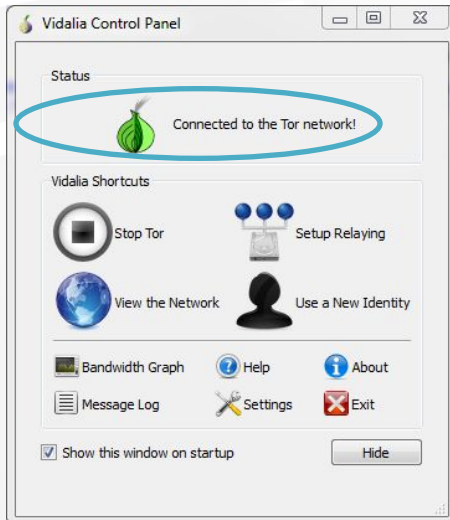
Anonymous Browsing - Tor



- 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

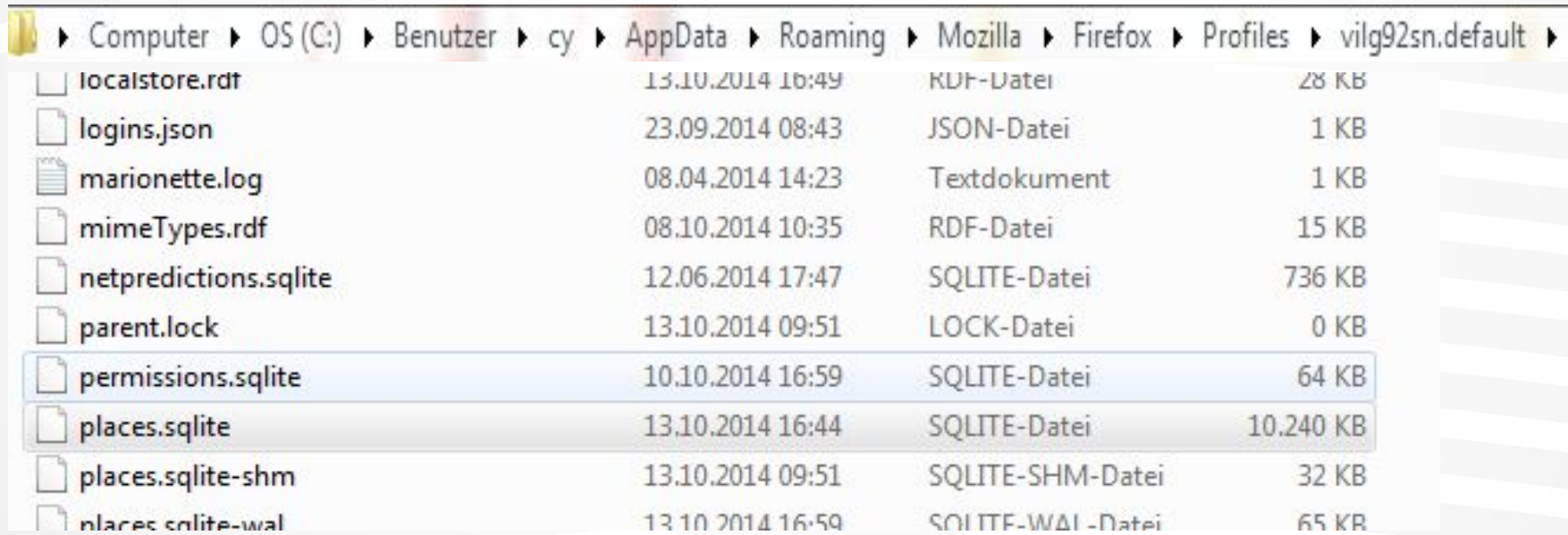
- **On Linux**

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



Firefox Practical

- Locate places.sqlite



| | | | |
|--|------------------|------------------|-----------|
| Computer > OS (C:) > Benutzer > cy > AppData > Roaming > Mozilla > Firefox > Profiles > vilg92sn.default | | | |
| localstore.rdf | 13.10.2014 16:49 | RDF-Datei | 28 KB |
| logins.json | 23.09.2014 08:43 | JSON-Datei | 1 KB |
| marionette.log | 08.04.2014 14:23 | Textdokument | 1 KB |
| mimeTypes.rdf | 08.10.2014 10:35 | RDF-Datei | 15 KB |
| netpredictions.sqlite | 12.06.2014 17:47 | SQLITE-Datei | 736 KB |
| parent.lock | 13.10.2014 09:51 | LOCK-Datei | 0 KB |
| permissions.sqlite | 10.10.2014 16:59 | SQLITE-Datei | 64 KB |
| places.sqlite | 13.10.2014 16:44 | SQLITE-Datei | 10.240 KB |
| places.sqlite-shm | 13.10.2014 09:51 | SQLITE-SHM-Datei | 32 KB |
| places.sqlite-wal | 13.10.2014 16:59 | SQLITE-WAL-Datei | 65 KB |



Firefox Practical

```
SELECT name, time, number FROM TABLE1
```

places.sqlite

TABLE 1

| |
|--------|
| name |
| time |
| number |
| value |
| value |
| value |
| value |

TABLE 2

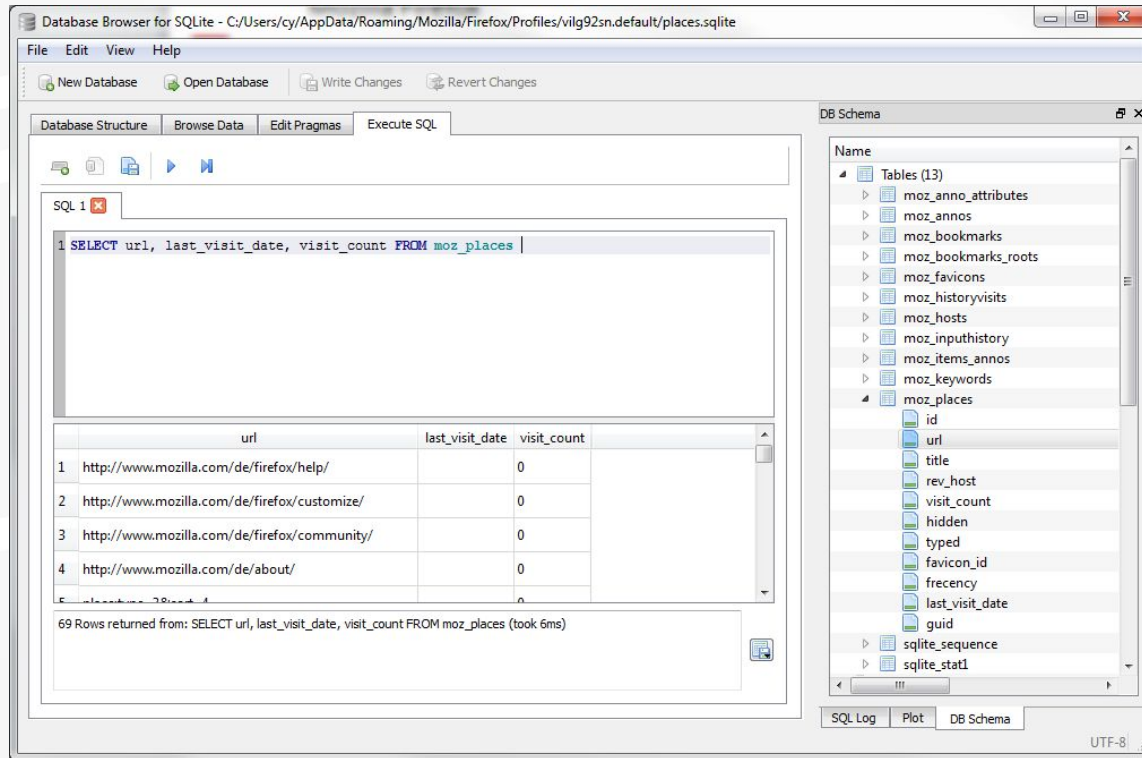
| |
|--------|
| name |
| time |
| number |
| value |
| value |
| value |
| value |



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

The screenshot shows the Database Browser for SQLite application. The main window displays the following SQL query and its results:

```
SQL 1  
1 SELECT title, dateAdded, lastModified from moz_bookmarks
```

| | title | dateAdded | lastModified |
|---|-------------------------|------------------|------------------|
| 1 | | 1351848837968000 | 1351848843334000 |
| 2 | Lesezeichen-Menü | 1351848837968000 | 1405065124573000 |
| 3 | Lesezeichen-Symboleiste | 1351848837968000 | 1409127236441000 |
| 4 | Schlagwörter | 1351848837968000 | 1351848837968000 |
| 5 | Unsortierte Lesezeichen | 1351848837968000 | 1411398842721000 |

83 Rows returned from: SELECT title, dateAdded, lastModified from moz_bookmarks (took 7ms)

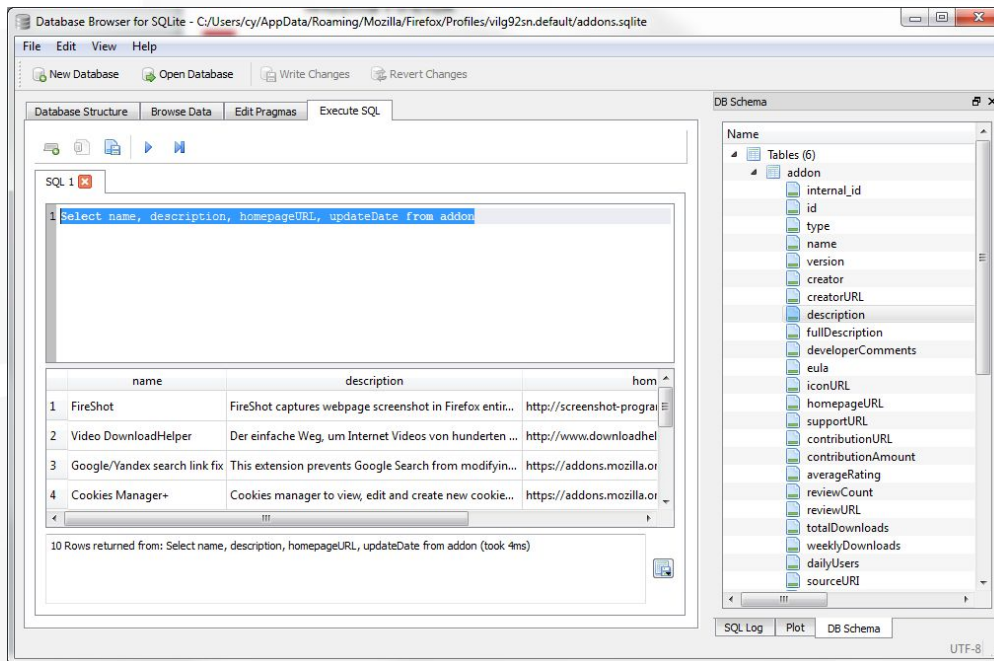
The right-hand pane shows the DB Schema for the database, listing 13 tables. The 'moz_bookmarks' table is expanded, showing its columns: id, type, fk, parent, position, title, keyword_id, folder_type, dateAdded, lastModified, and guid.



Firefox Practical

- AddOns

SELECT name, description, homepageURL, updateDate FROM addon



Firefox Practical

- Form data

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

The screenshot shows the Database Browser for SQLite interface. The main window displays the following SQL query:

```
1 Select fieldname, value, timesUsed, firstUsed, lastUsed from moz_formhistory
```

The results are shown in a table with the following data:

| | fieldname | value | timesUsed | firstUsed | lastUsed |
|---|-----------|-----------------------|-----------|------------------|------------------|
| 1 | email | yesil.cemil@gmail.com | 2 | 1413190475378000 | 1413210845919000 |
| 2 | Email | yesil.cemil | 1 | 1413200324437000 | 1413200324437000 |
| 3 | name | cemil | 1 | 1413211060841000 | 1413211060841000 |
| 4 | name | cemilz/MbA | 1 | 1413211073253000 | 1413211073253000 |
| 5 | name | yesil.cemil@gmail.com | 1 | 1413211081322000 | 1413211081322000 |

5 Rows returned from: Select fieldname, value, timesUsed, firstUsed, lastUsed from moz_formhistory (took 4ms)

The right-hand pane shows the DB Schema for the moz_formhistory table, listing columns: id, fieldname, value, timesUsed, firstUsed, lastUsed, and guid. It also shows three indices: moz_formhistory_guid_index, moz_formhistory_index, and moz_formhistory_lastused_index.

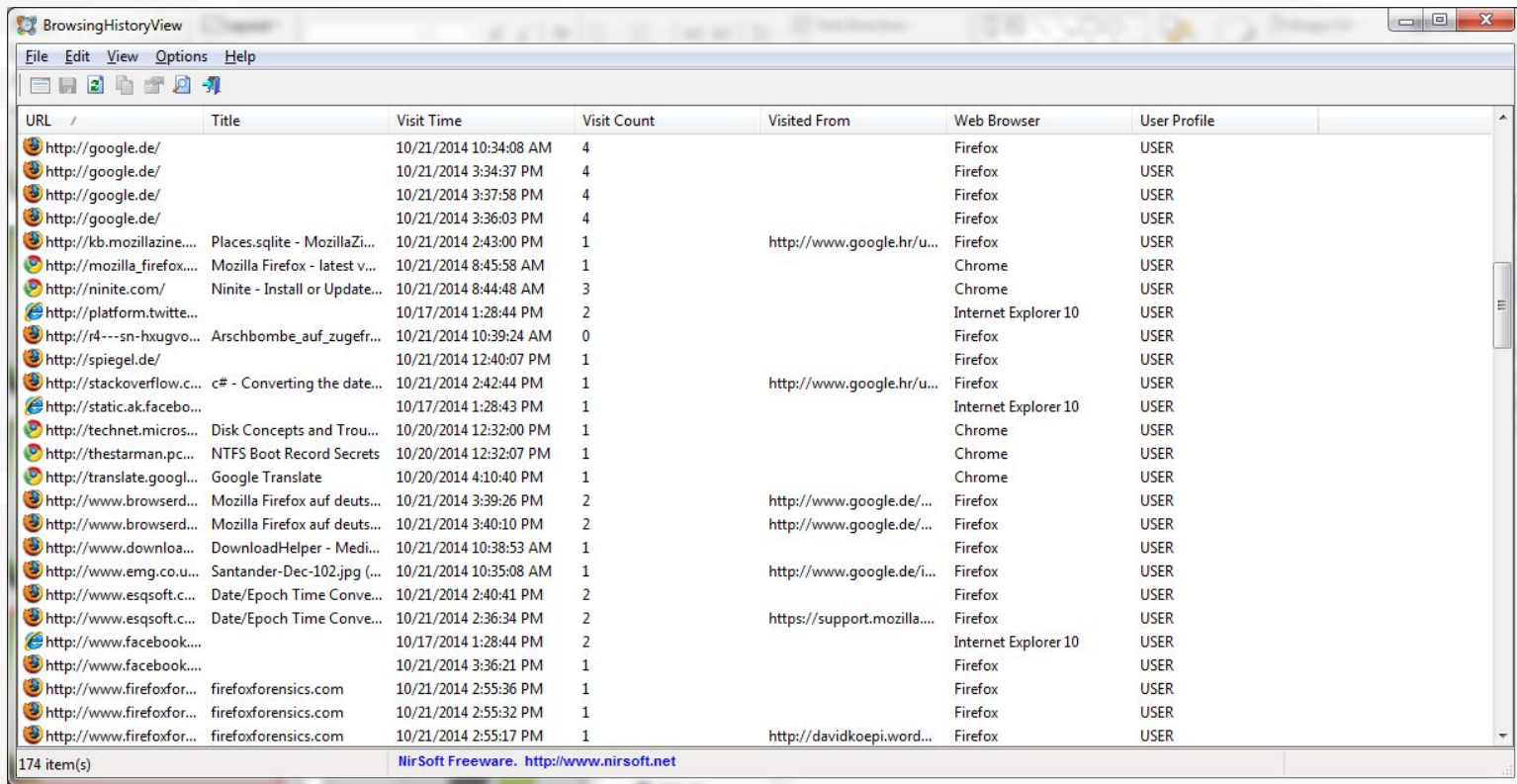


Firefox Practical

Tools

FreeTools

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



The screenshot shows the Nirsoft BrowsingHistoryView application window. The window title is "BrowsingHistoryView" and it has a menu bar with "File", "Edit", "View", "Options", and "Help". Below the menu bar is a toolbar with various icons. The main area displays a table of browser history items. The table has the following columns: URL, Title, Visit Time, Visit Count, Visited From, Web Browser, and User Profile. The table contains 174 items, with the first few rows showing visits to google.de and various other websites. The status bar at the bottom indicates "174 item(s)" and "NirSoft Freeware. <http://www.nirsoft.net>".

| URL | Title | Visit Time | Visit Count | Visited From | Web Browser | User Profile |
|----------------------------|-------------------------------|------------------------|-------------|----------------------------|----------------------|--------------|
| http://google.de/ | | 10/21/2014 10:34:08 AM | 4 | | Firefox | USER |
| http://google.de/ | | 10/21/2014 3:34:37 PM | 4 | | Firefox | USER |
| http://google.de/ | | 10/21/2014 3:37:58 PM | 4 | | Firefox | USER |
| http://google.de/ | | 10/21/2014 3:36:03 PM | 4 | | Firefox | USER |
| http://kb.mozillazine.... | Places.sqlite - MozillaZi... | 10/21/2014 2:43:00 PM | 1 | http://www.google.hr/u... | Firefox | USER |
| http://mozilla_firefox.... | Mozilla Firefox - latest v... | 10/21/2014 8:45:58 AM | 1 | | Chrome | USER |
| http://ninite.com/ | Ninite - Install or Update... | 10/21/2014 8:44:48 AM | 3 | | Chrome | USER |
| http://platform.twitte... | | 10/17/2014 1:28:44 PM | 2 | | Internet Explorer 10 | USER |
| http://r4---sn-hxugvo... | Arschbombe_auf_zugefr... | 10/21/2014 10:39:24 AM | 0 | | Firefox | USER |
| http://spiegel.de/ | | 10/21/2014 12:40:07 PM | 1 | | Firefox | USER |
| http://stackoverflow.c... | c# - Converting the date... | 10/21/2014 2:42:44 PM | 1 | http://www.google.hr/u... | Firefox | USER |
| http://static.ak.facebo... | | 10/17/2014 1:28:43 PM | 1 | | Internet Explorer 10 | USER |
| http://technet.micros... | Disk Concepts and Trou... | 10/20/2014 12:32:00 PM | 1 | | Chrome | USER |
| http://thestarman.pc... | NTFS Boot Record Secrets | 10/20/2014 12:32:07 PM | 1 | | Chrome | USER |
| http://translate.googl... | Google Translate | 10/20/2014 4:10:40 PM | 1 | | Chrome | USER |
| http://www.browserd... | Mozilla Firefox auf deuts... | 10/21/2014 3:39:26 PM | 2 | http://www.google.de/... | Firefox | USER |
| http://www.browserd... | Mozilla Firefox auf deuts... | 10/21/2014 3:40:10 PM | 2 | http://www.google.de/... | Firefox | USER |
| http://www.downloa... | DownloadHelper - Medi... | 10/21/2014 10:38:53 AM | 1 | | Firefox | USER |
| http://www.emg.co.u... | Santander-Dec-102.jpg (...) | 10/21/2014 10:35:08 AM | 1 | http://www.google.de/i... | Firefox | USER |
| http://www.esqsoft.c... | Date/Epoch Time Conve... | 10/21/2014 2:40:41 PM | 2 | | Firefox | USER |
| http://www.esqsoft.c... | Date/Epoch Time Conve... | 10/21/2014 2:36:34 PM | 2 | https://support.mozilla... | Firefox | USER |
| http://www.facebook... | | 10/17/2014 1:28:44 PM | 2 | | Internet Explorer 10 | USER |
| http://www.facebook... | | 10/21/2014 3:36:21 PM | 1 | | Firefox | USER |
| http://www.firefoxfor... | firefoxforensics.com | 10/21/2014 2:55:36 PM | 1 | | Firefox | USER |
| http://www.firefoxfor... | firefoxforensics.com | 10/21/2014 2:55:32 PM | 1 | | Firefox | USER |
| http://www.firefoxfor... | firefoxforensics.com | 10/21/2014 2:55:17 PM | 1 | http://davidkoepi.word... | Firefox | USER |



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\\gx\\Desktop\\Hacker");
user_pref("browser.download.manager.alertOnEXEOpen", true);
user_pref("browser.download.panel.firstSessionCompleted", true);
```



Privatmode

No history is stored

