Browser Forensics Analysis is a separate, large area of expertise.

Web browsers are used in mobile devices, tablets, netbooks, desktops, etc., and often can be used not just for web surfing, but for navigation through the file system of the device. The web browser's cache can contain downloaded images, videos, documents, executable files and scripts. Web browsers also can contain data entered into forms: search queries, logins and passwords for web email accounts, social networks, other web sites and financial information (for example, credit card numbers). Favorites and searches can give the researcher an idea of the device owner's interests.

Browser Forensics is of no small importance in incident response for understanding how an attack on a computer or computer network began and finding the source of compromise.

The main sources of malware / spyware / adware are emails (including web mails), social networks and other compromised sites. Typically, a user accesses all these sources (web emails, social networks, sites) using web browsers.

Web browsers overview

One of the most famous web browsers is Internet Explorer. This browser is a component of the Windows operating system and is often used as a default web browser. In Windows 10, Microsoft replaced Internet Explorer with Microsoft EDGE. Microsoft EDGE is a web browser that contains new features. Microsoft plans to replace Internet Explorer with Microsoft EDGE on all devices, including Android and iOS mobile devices. Internet Explorer and Microsoft EDGE can work in InPrivate mode, without storing information about web resources visited by the user.

Another popular web browser is Google Chrome. It has the following features:

- Integration with Google services.
- Synchronization of user passwords between devices.
- The ability to use extensions and plugins.
- Fast operation.
- Gathers user data.
- Consumes large amounts of memory.

Google Chrome can work in Incognito mode, which prevents the browser from permanently storing any history information, cookies, site data or form inputs.

Third-party developers have created a huge number of web browsers based on the Chrome Engine, such as: 360 Extreme Explorer, Avast SafeZone, Chromium, Comodo Dragon, CoolNovo, Cốc Cốc, Epic Browser, Flock, Vivaldi, Rockmelt, Sleipnir, SRWare Iron, Titan Browser, Torch Browser, Yandex.Browser, Opera, Orbitum, Breach, Nihrome, Perk, QIP Surf, Baidu Spark, Uran, Chromodo, Sputnik, Amigo, etc.

All these browsers have functionality similar to Google Chrome and produce web browser artifacts like Google Chrome. These browsers support most of Google Chrome’s extensions and plugins.

One of the most famous web browsers with the Google Chrome engine is Opera. Opera was the first to introduce features that other web browsers adopted: Speed Dial, pop-up blocking, re-opening recently closed pages, private browsing and tabbed browsing. Also, Opera contains a free Virtual Private Network (VPN) service, which allows users to surf the web anonymously.

Firefox is a fairly popular web browser, with artifacts that can be found on devices under investigation. This web browser has the following features:

- More secure (compared to other browsers).
- Advanced Incognito mode, disabling tracking of user's locations and advertisements.
- Has its own extensions.

Gecko is a browser engine developed by Mozilla. It is used in the Firefox browser, the Thunderbird email client and many other projects.

Based on Gecko, third-party developers have created various web browsers: Firefox, Waterfox, Cyberfox, SeaMonkey, Netscape Navigator, CometBird, BlackHawk, IceCat, IceDragon, Pale Moon, Flock, K-Meleon, Galeon, FlashFox, Orfox, Vega.

Chinese Web Browsers

The most popular Chinese web browsers are: Qihoo 360 Secure Browser, Baidu Browser (c 2011), Tencent QQ Browser, Sogou browser, Maxthon, UC browser. As a rule, these browsers are based on the Chrome Engine, it has insufficient protection, are perceived by antivirus software as adware. The Chinese web browsers are based on Google Engine. Usually these browsers have integrated extensions and plugins that have spyware and adware functionality, so antivirus software detects the browsers like spyware or adware. Also, these web browsers often collect data about users.

Encryption of data

Part of the data in web browsers is encrypted (for example, passwords to websites). Internet Explorer on Microsoft EDGE uses the Data Protection Application Programming Interface. The DPAPI mechanism appeared in

Windows 2000 and is used to protect stored passwords and confidential information on the computer. This mechanism includes the functions of encryption and decryption of data and RAM.

You need a user password to decrypt the encrypted data. If the password is logged into your account using the login and the password, the operating system uses the hash of the password to decrypt the encrypted data.

As a rule, data encryption is carried out using the SHA1 algorithm, however, in some cases, the data is encrypted using a less crypto-resistant algorithm.

Difficulties of web browsers forensic analysis

An examiner can have the following difficulties when analyzing web browsers:

- Many browsers, lots of data
- Different data
- Encryption used to protect user data
- User’s use of Private mode (or Incognito mode), in which the examined computer does not have web browser artifacts.

Web browser forensic artifacts

Of course, each web browser leaves its own individual artifacts in the operating system. Types of artifacts from the web browser can vary depending on the version of the web browser. Typically, when researching artifacts of web browsers, you can extract the following types of artifacts:

- History
- Cache
- Cookies
- Typed URLs
- Sessions
- Most visited sites
- Screenshots
- Financial info

- Form values (Searches, Autofill)
- Downloaded files (Downloads)
- Favorites

Cookies

Cookies are text files used to give feedback from the user to the server. When performing some actions with a web resource (viewing web links, downloading files, etc.), these actions are registered in a cookie that is secretly sent by the server to the user's computer. With this web resource, the server has the ability to find out what actions the user has taken on previous visits to this web resource.

\Windows\Cookies\ (Windows 98) (Internet Explorer)

\Documents and Settings\Administrator\Cookies (Windows 2000, Windows XP) (Internet Explorer)

\Users\%userprofile%\AppData\Roaming\Microsoft\Windows\Cookies (Windows 7) (Internet Explorer)

\Users\Default\AppData\Roaming\Microsoft\Windows\Cookies (Windows 7) (Internet Explorer)

\Users\%userprofile%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat (Microsoft EDGE, Windows)

\Users\%userprofile%\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\#!002\MicrosoftEdge\Cookies\XXXXXXXX.cookie (or XXXXXXXX.txt file) (Microsoft EDGE, Windows)

\Users\%userprofile%\AppData\Local\Microsof\Windows\INetCookies\ (Microsoft EDGE, Windows)

\Users\%userprofile%\AppData\Local\Microsof\Windows\INetCookies\Low\ (Microsoft EDGE, Windows)

\Users\%userprofile%\AppData\Local\Packages\microsof.microsofedge_8wekyb3d8bbwe\AC\#!121\MicrosofEdge\Cookies\ (Microsoft EDGE, Windows)

\Users\%userprofile%\AppData\Local\Packages\microsof.microsofedge_8wekyb3d8bbwe\AC\MicrosofEdge\Cookies\ (Microsoft EDGE, Windows)

\Users\%userprofile%\AppData\Local\Packages\microsof.microsofedge_8wekyb3d8bbwe\AC\#!002\MicrosofEdge\Cookies\ (Microsoft EDGE, Windows)

\Users\%userprofile%\AppData\Local\Packages\microsof.microsofedge_8wekyb3d8bbwe\AC\#!001\MicrosofEdge\Cookies\ (Microsoft EDGE, Windows)

\Users\%userprofile%\AppData\Local\Packages\Microsof.SkypeApp_kzf8qxf38zg5c\AC\INetCookies\

Cache
\Users\%userprofile%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat (Microsoft EDGE, Windows)

\Users\%userprofile%\AppData\Local\Packages\microsof.microsofedge_8wekyb3d8bbwe\AC\MicrosofEdge\Cache\xxxxxxxx\ (Microsoft EDGE, Windows)

\Users\%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\cookies.sqlite (Firefox, Windows)

\Users\%userprofile%\AppData\Local\Google\Chrome\User Data\Default\Cookies.db (Google Chrome, Windows)

Cache

Users\%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\cache2\entries Firefox (Windows)

\Users\%userprofile%\AppData\Local\Google\Chrome\User Data\Default\Cache\ (Google Chrome, Windows)

\Users\%userprofile%\AppData\Local\Google\Chrome\User Data\Default\GPUCache\ (Google Chrome, Windows)

\Users\%userprofile%\AppData\Local\Google\Chrome\User Data\Default\Media Cache\ (Google Chrome, Windows)

\Users\%userprofile%\AppData\Roaming\Opera Software\Opera Stable\ShaderCache\GPUCache\data_3 (Opera, Windows)

\Users\%userprofile%\Library\Caches\com.apple.Safari\Cache.db (Safari, MacOS)

Favorites

\Users\%userprofile%\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\MicrosoftEdge\User\Default\DataStore\Data\ nouser1\120712-0049\BDStore (for later versions) (Microsoft EDGE, Windows)

\Users\%userprofile%\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\MicrosoftEdge\User\Default\Favorites (for early versions) (Microsoft EDGE, Windows)

\Users\%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\places.sqlite (Firefox, Windows)

\Users\%userprofile%\AppData\Local\Google\Chrome\User Data\Default\Bookmarks (Google Chrome, Windows)

\Users\%userprofile%\Library\Safari\Bookmarks.plist (Safari, MacOS)

Session

\Users\%userprofile%\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\MicrosoftEdge\User\Default\Recovery\Active\{07677C23-6987-4777-B133-5AC24BD039F5}.dat (Microsoft EDGE, Windows)

\Users\%userprofile%\AppData\Roaming\Opera Software\Opera Stable\Current Session (Opera, Windows)

Session Recovery

\Users\%userprofile%\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\MicrosoftEdge\User\Default\Recovery\Active\{A7D7A4FC-7458-11E6-9BCD-000C29566E3E}.dat (Microsoft EDGE, Windows)

\Users\%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\sessionstore.js

(Firefox, Windows)

Downloaded files

\Users\%userprofile%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat (Microsoft EDGE, Windows)

\Users\%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\places.sqlite (Firefox, Windows)

\Users\%userprofile%\AppData\Local\Google\Chrome\User Data\Default\History (Google Chrome, Windows)

URLs

\Users\%userprofile%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat (Microsoft EDGE, Windows)

\Users\%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\places.sqlite (Firefox, Windows)

\Users\%userprofile%\AppData\Local\Google\Chrome\User Data\Default\History (Google Chrome, Windows)

\Users\%userprofile%\Library\Safari\History.db (Safary, MacOS)

Form values

\Users\%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\formhistory.sqlite (Firefox, Windows)

\Users\%userprofile%\AppData\Local\Google\Chrome\User Data\Default\Web Data (Google Chrome, Windows)

Typed URLs

\Users\%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\places.sqlite (Firefox, Windows)

\Users\%userprofile%\AppData\Local\Google\Chrome\User Data\Default\History (Google Chrome, Windows)

Session Store Artifacts

\Users\%userprofile%\Library\Safari\LocalStorage\ (Firefox, Windows)

Searches

\Users\%userprofile%\AppData\Local\Google\Chrome\User Data\Default\Web Data (Google Chrome, Windows)

Most Visited sites

\Users\%userprofile%\Library\Safari\TopSites.plist (Safari, MacOS)

Last Session

\Users\%userprofile%\AppData\Local\Google\Chrome\User Data\Default\Last Session (Google Chrome, Windows)

\Users\%userprofile%\AppData\Roaming\Opera Software\Opera Stable\Last Session (Opera, Windows)

\Users\%userprofile%\Library\Safari\LastSession.plist (Safari, MacOS)

Last Tabs

\Users\%userprofile%\AppData\Local\Google\Chrome\User Data\Default\Last Tabs (Google Chrome, Windows)

\Users\%userprofile%\AppData\Roaming\Opera Software\Opera Stable\Last Tabs (Opera, Windows)

Current Tabs

\Users\%userprofile%\AppData\Local\Google\Chrome\User Data\Default\Current Tabs (Google Chrome, Windows)

\Users\%userprofile%\AppData\Roaming\Opera Software\Opera Stable\Current Tabs (Opera, Windows

Current Session

\Users\%userprofile%\AppData\Local\Google\Chrome\User Data\Default\Current Session (Google Chrome, Windows)

How is the data stored?

Internet Explorer and Windows Explorer store most of the data in index.dat files.

INDEX.DAT files are used by Internet Explorer to store information about visited pages, cookies and the time they are used. To this end, Internet Explorer indexes files that are located in folders that are browser caches and maps these files to the network resource from which these files were downloaded. In addition, INDEX.DAT files contain such information as the decryption of HTTP-header packets, in which the file was transferred, the date of creation and last access to the file, the number of calls to it, and much more.

\Documents and Settings\%userprofile%\Local Settings\Temporary Internet Files\Content.IE5\index.dat

\Users\%userprofile%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat

\Documents and Settings\%userprofile%\Cookies\

\Documents and Settings\%userprofile%\Local Settings\History\History.IE

\Documents and Settings\%userprofile%\Local Settings\History\History.IE\MSHist[timestamps]

Google Chrome, Safari, Firefox, Opera store most of the data in SQLite databases. Manual analysis of these databases and carving will allow you to extract the maximum amount of data.

When analyzing SQLite data bases, remember:

- Some deleted records can be found in Freelist – unused tables that can contain deleted data.

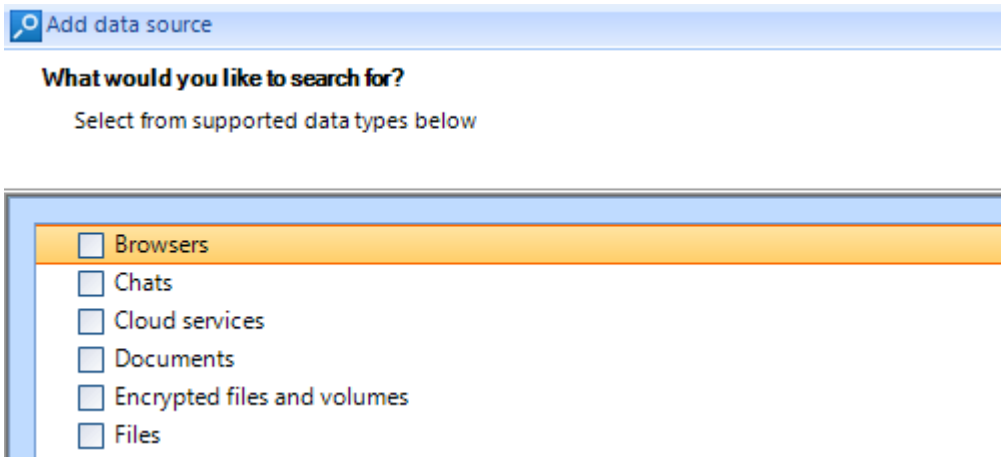
Where can I find the Web Browsers artifacts?

- Physical dumps of mobile devices.
- File systems of mobile devices.
- Backups of mobile devices.
- Data, which can be extracted from Clouds.
- Hard drives.
- Images of hard drives.

- Memory dumps.
- Hibernation and page files.

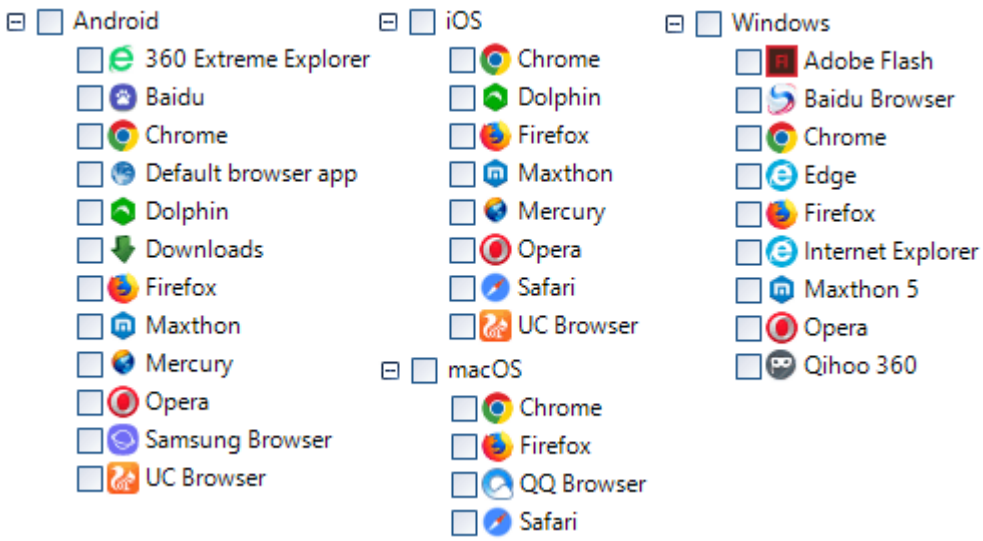
Belkasoft Features

Belkasoft can analyze carving and extract web browsers artifacts from all the data sources mentioned above.



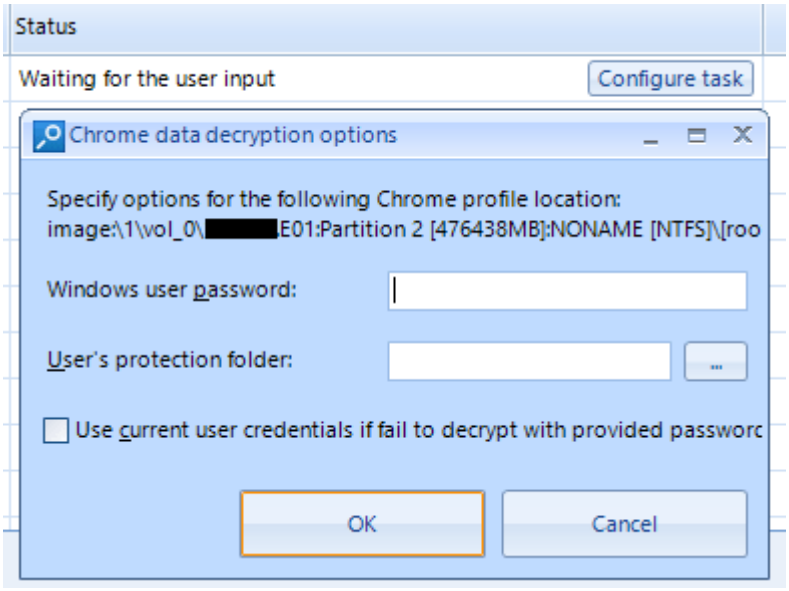
Supported operating systems:

- Android
- iOS
- MacOS
- Windows

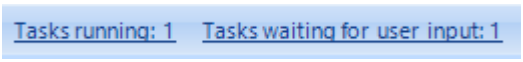


* This list is not exhaustive.

If during the processing of the case encrypted data is found (for example, user passwords from web sites) an examiner will be prompted to enter the Windows user password to decrypt such data. The window for entering this password is in the Task Manager tab.

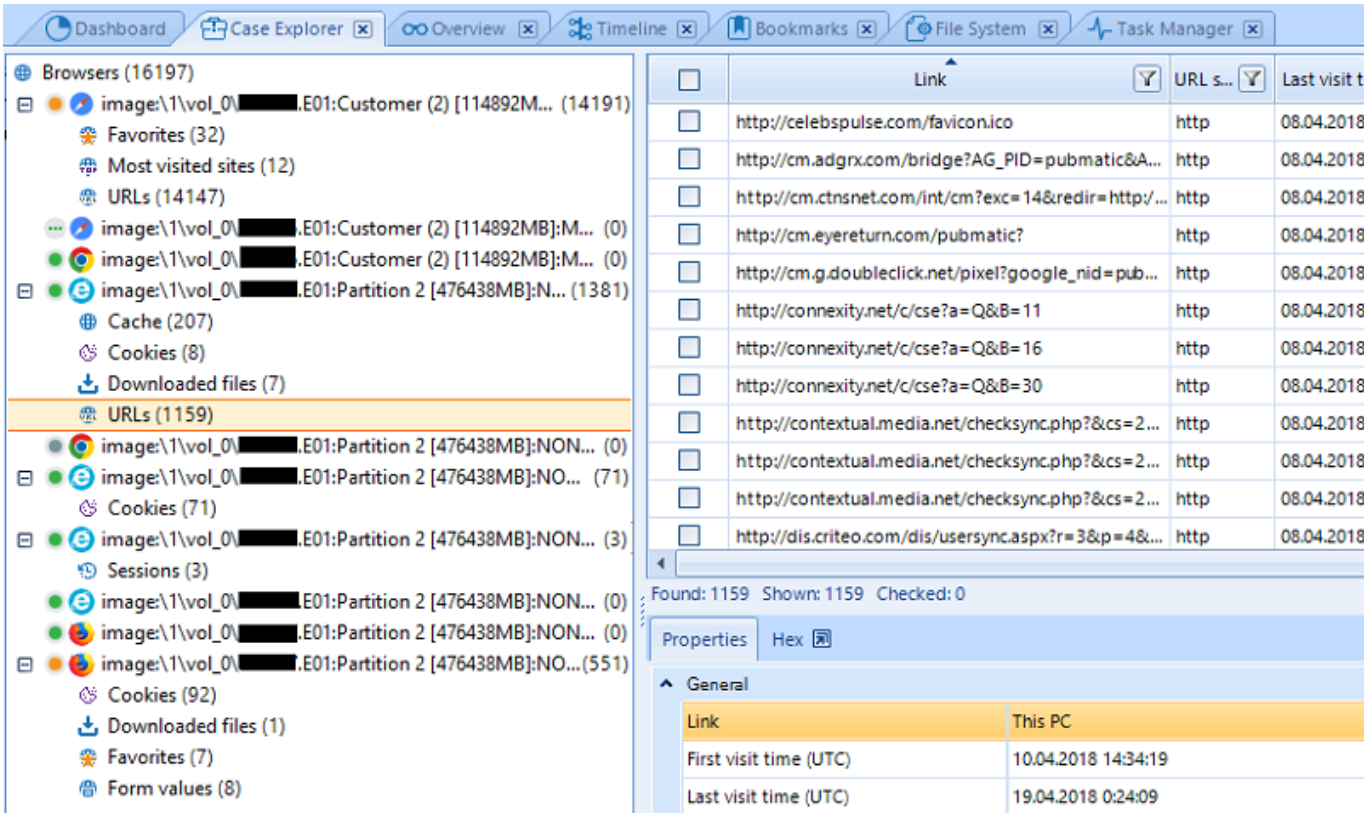


The fact that you need to enter the Windows user password informs the Task waiting for user input: … line that appears in the lower right corner of the main program window.

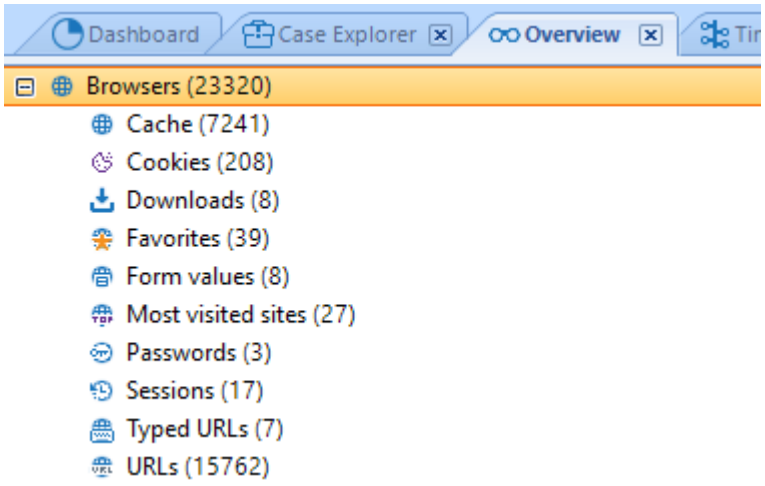


The analysis results will be displayed in the Case Explorer and Overview tabs after processing the sources.

To view the various web browser artifacts in Case Explorer, click the '+' symbol opposite the selected source. In this case, in the Case Explorer tab, the categories of artifacts extracted from this source will be displayed.

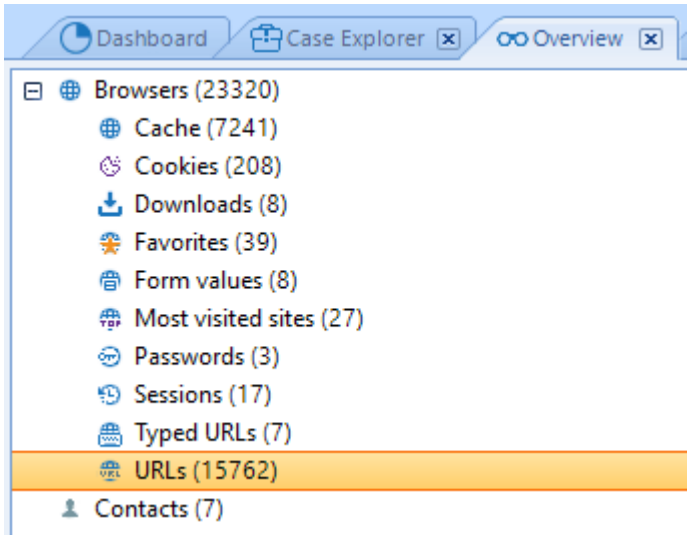


Information about discovered Web Browsers artifacts displayed in the Overview tab.

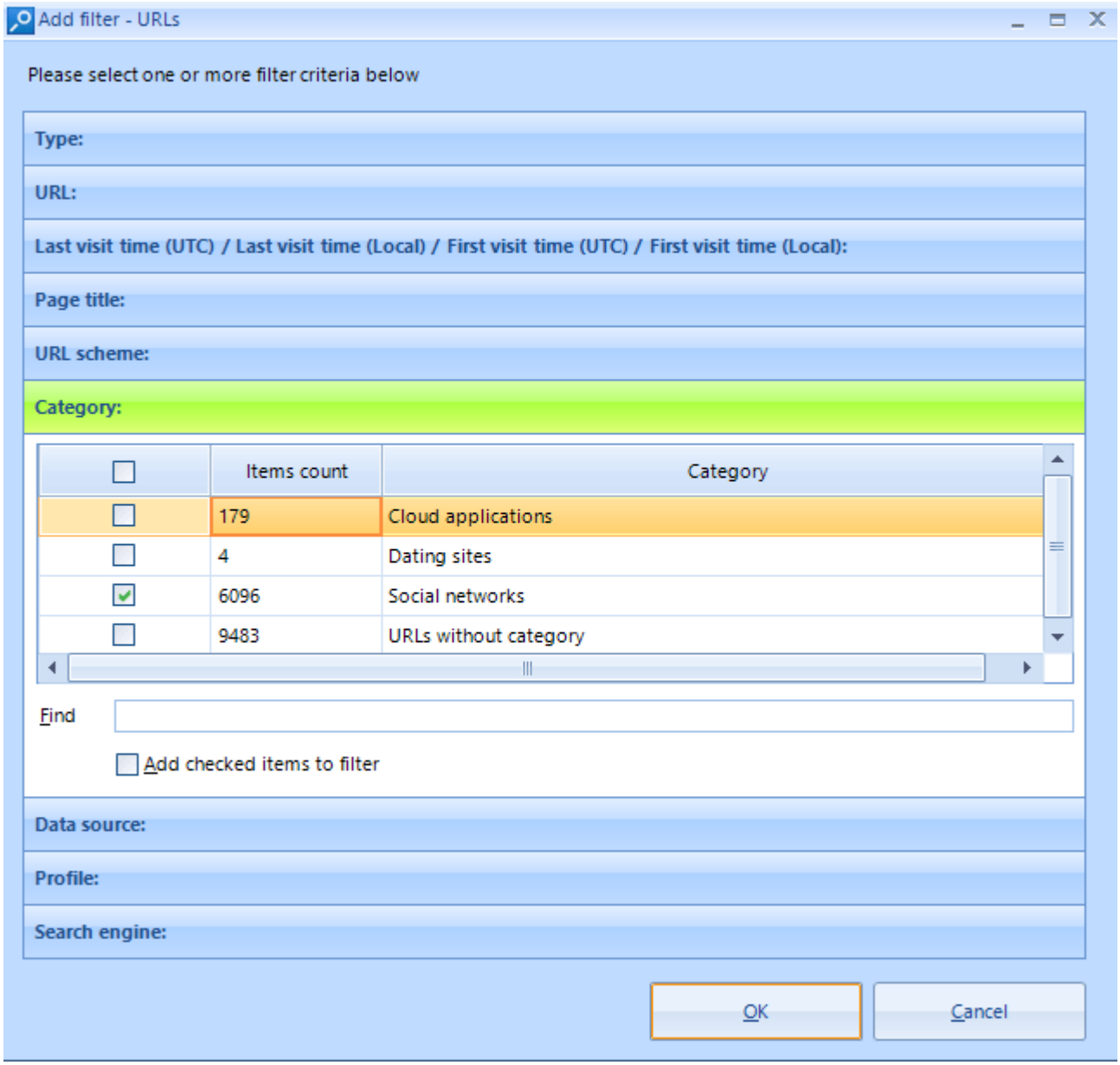


Filters

The extracted web history can be sorted by categories. To do this, select the category of URLs artifacts in the Overview tab.



Click the Add filter button on the filter panel. Select Category: and in it the category you are interested in the Add filter -URLs window. Click the OK button.



As a result, in the main Belkasoft Evidence Center window only social networks URLs will be displayed.

Questions

What is browser forensics?

state and explain difficulties in browser forensics.

How data is stored in browser forensics.

explain web browsing activity reconstruction.