New Artefacts in v2.8

Introduction

This version of NetAnalysis® introduces support for two new browsers as well as adding support for the latest release versions of existing browsers which are already supported.

Some notable new features include support for decrypting the logins and passwords from the latest Mozilla based browsers as well as processing Mozilla session and search engine files. We have also added support for Microsoft Edge backups and Apple Safari recently closed tabs, last session files, user notification permissions and search descriptions.

Some improvements to the software include DirectX hardware acceleration support for the data grid which increases performance. We have also added the ability to save data stored in encoded data URLs.

New Browser Support

We have added support for the following browsers:

AOL Desktop Browser v9

AOL Desktop was an Internet suite produced by AOL which contained an integrated web browser. Prior to version 9.8, the browser was based on the Trident layout engine as used by Internet Explorer. From v9.8 onward, Trident was replaced with CEF (Chromium Embedded Framework) to provide users with a more modern browsing experience. Despite AOL Desktop being discontinued in 2018, it is still encountered during investigations.

Blisk Browser v0 - 8

Blisk is a Chromium based web browser which has been designed to be used by web developers. It provides an array of tools for web development and testing across a number of different devices. It contains a pre-installed set of emulation tools for testing phones, tablets, laptop and desktop devices. This makes it a simple task for web developers to test how their code renders across multiple devices, browsers and screen resolutions.

Updated Support for Existing Supported Browsers

NetAnalysis® currently supports a wide variety of desktop and mobile browsers. There have been a number of changes to the currently supported browsers. Here are some of these changes:

Login and Password Decryption

A recent change to the encryption/decryption methodology for Firefox Desktop browsers resulted in the process requiring access to a new file called key4.db; using this file matches the behaviour of some mobile versions of the browser. NetAnalysis® supports the decryption of login information and passwords using both key store files.

New Support for Existing Browsers

To enhance our support for existing web browsers, we have added the following:

Mozilla Session Stores

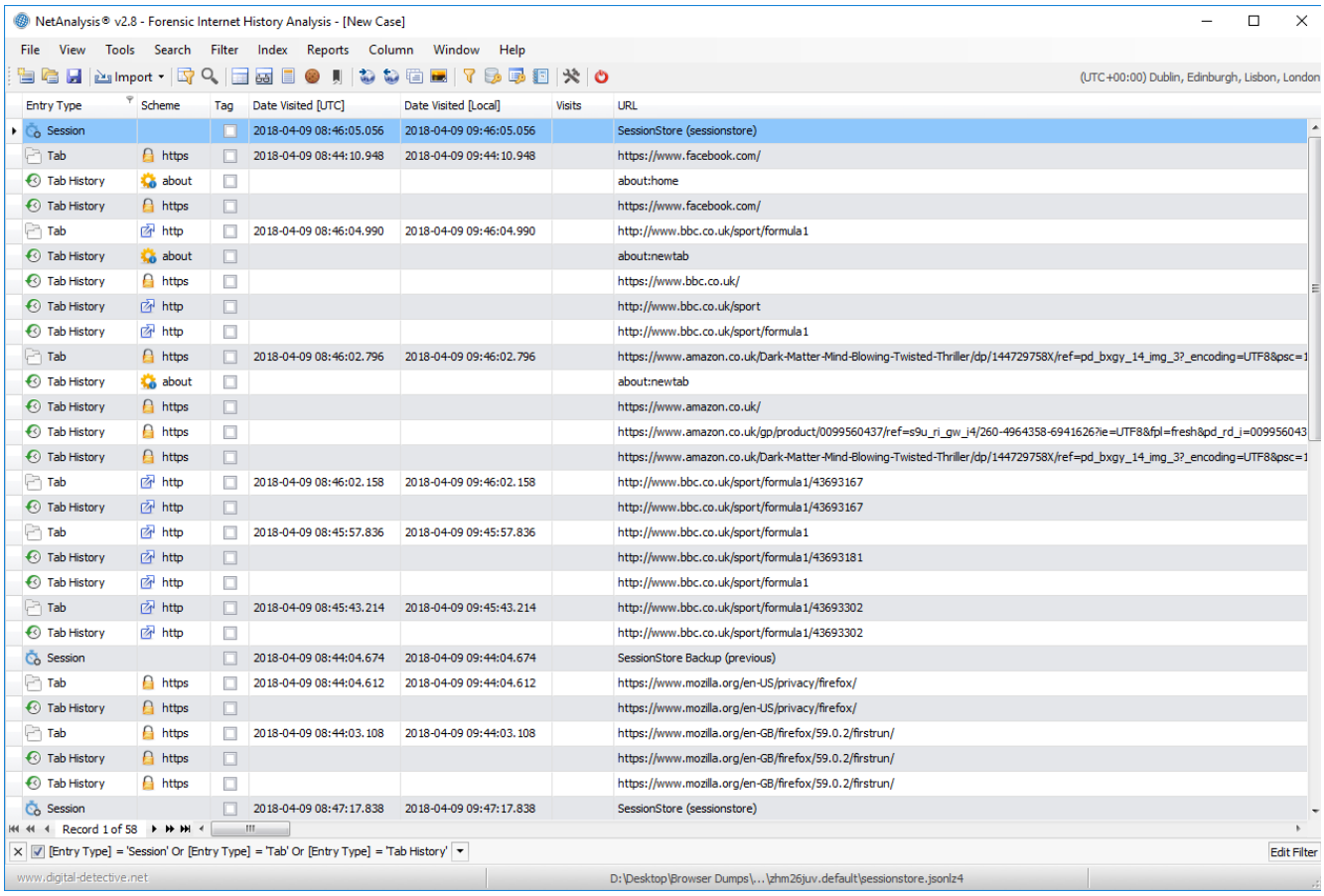
Mozilla Firefox and many of the Mozilla based browsers store session information relating to the state of a user's browsing session so that the windows and tabs that were open when the browser was last closed, terminated unexpectedly or a software update applied can be restored.

There are usually multiple versions of a user's session store file located in the user profile folder with backup copies saved to the sessionstore-backups folder. Session store files have different file names depending on how the browser uses them during the session restore process:

- sessionstore,
- recovery,
- previous,
- upgrade.

As well as information on the currently open windows and tabs, a session store file also stores information on recently closed windows and tabs and cookies relating to the saved session. In the more recent versions of Firefox these session store files are now saved in a compressed format.

NetAnalysis® now recovers all versions of Mozilla based session store files.



Mozilla Search Engine Data

Mozilla Firefox and many of the Mozilla based browsers store their search engine data in a JSON format search file. This includes the default search engines that come preinstalled with the browser and user installed search engines and search engine add-ons. The user can then choose to search with one of these alternative search engine rather than the default. In the most recent versions of Firefox the search engine file is now saved in a compressed format.

We have added support for the import of all versions of this file to NetAnalysis®.

Microsoft Edge Backups

Microsoft Edge recently added a feature to create an automatic backup of the user's 'favourite' entries using the Netscape bookmark file format. NetAnalysis® can identify and import these files.

Apple Safari Search Descriptions

Quick Website Search was a feature added to Safari v8. If a website includes an OpenSearch description document, the site can be identified by the browser as having searchable content. The first time a user visits such a website, Safari will add it to the Manage Websites panel of Safari's Search Preferences. The user can then access content from this website directly from Safari's Smart Search field thus bypassing their normal search engine. Safari stores this Quick Website Search information in a SearchDescriptions.plist file.

NetAnalysis® now recovers Safari Quick Website Search information.

Apple Safari User Notification Permissions

Safari allows the user to manage website push notifications. The list of websites that have asked for permission to display alerts can be viewed in Safari's Notifications Preferences. Each website has an option to allow or deny the push notifications.

NetAnalysis® now recovers this information and details the notification permission setting to the Information panel.

Apple Safari Last Session

All versions of Safari v3+ on both Mac OS X and Windows contain a LastSession.plist file which records the current state of the browser. Safari can use this file to reopen all the windows and tabs which were open the last time the browser closed or terminated unexpectedly. The Safari menu item Reopen All Windows from Last Session allows the user to do this manually.

Apple Safari Recently Closed Tabs

Apple Safari v10+ keeps track of recently closed tabs in a RecentlyClosedTabs.plist file. This allows the user to reopen closed tabs using the Recently Closed Safari menu item.

We have added support for the import of Last Session and Recently Closed Tabs into NetAnalysis®.

New Features

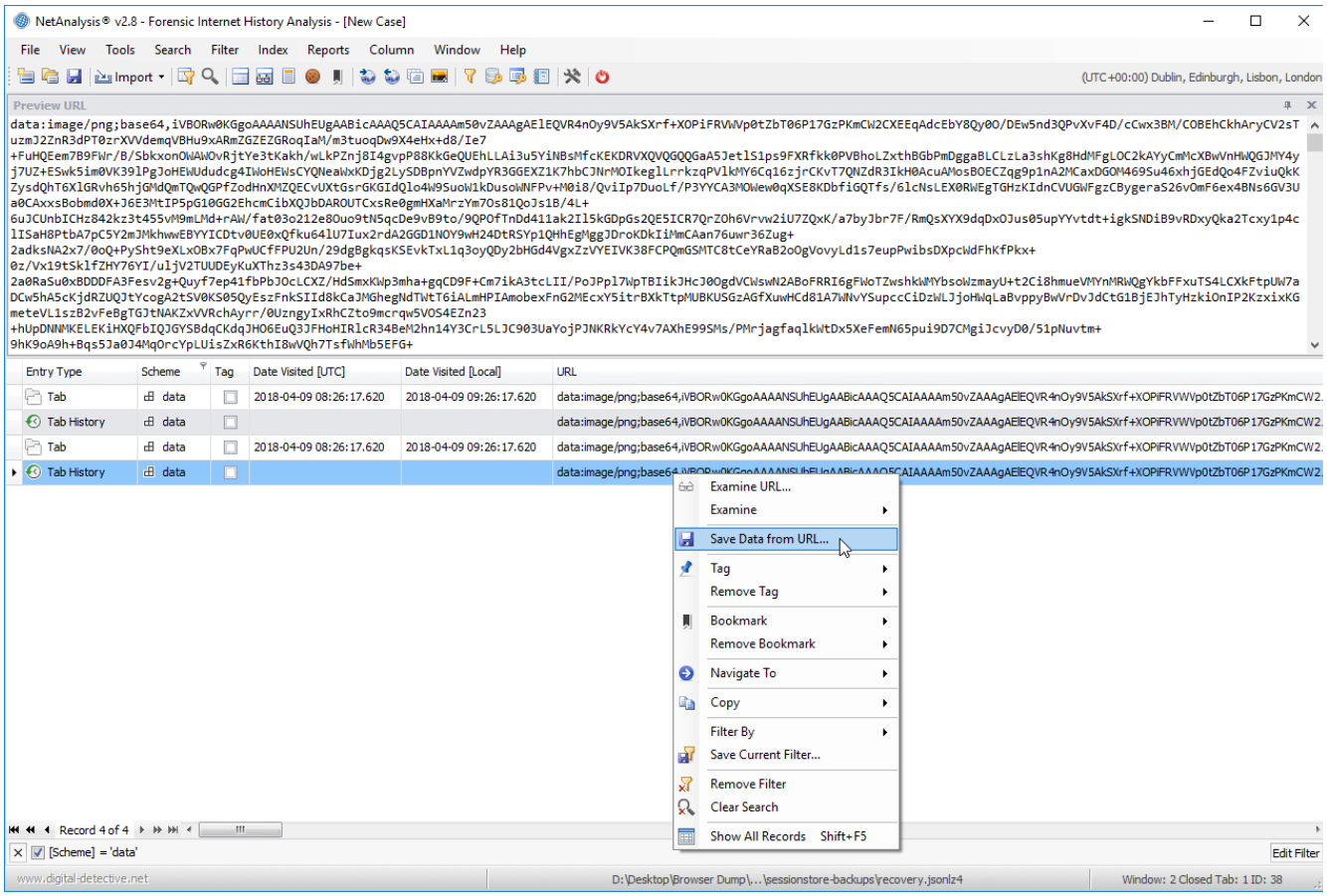
We have added some new features to NetAnalysis®:

Saving Data from Encoded Data URLs

Data URLs are prefixed with the data: scheme and allow content creators to embed small files inline in documents. They are composed of four parts: a prefix (data:), a MIME type indicating the type of data stored, an optional base64 token if the data is non-text, and the data itself:

```
data:[<mediatype>][;base64],<data>
```

Right clicking on the data URL allows the user to select **Save Data from URL**, this will show a Save File window prompting the user to select a location and file name. The decoding engine will automatically identify the correct file extension based on the source data.



DirectX Hardware Acceleration Support

In this release of NetAnalysis®, we have added support for DirectX hardware acceleration. This allows us to employ the client machine's video card (integrated or dedicated) to render the data grid. DirectX acceleration provides us with an incredible speed boost. If the source system is unable to provide the resources for DirectX painting, the application will revert to GDI+ rendering.