New Artefacts in v2.9

Introduction

This release of NetAnalysis® adds support for Basilisk Browser, Epic Privacy Browser, Cc Cc Browser and QQ Browser. We have also improved support for many of the existing browsers.

Some notable new features include the update of our internal HTML Viewer, as well as adding some valuable new functionality to aid with evidence processing and productivity.

New Browser Support

We have added support for the following browsers:

Basilisk

Basilisk is a free and Open Source XUL-based web browser, featuring the well-known Firefox-style interface and operation, created by the developers of the Pale Moon browser. It is based on the Goanna layout and rendering engine (a fork of Gecko) and builds on the Unified XUL Platform (UXP), which in turn is a fork of the Mozilla code base.

The developers describe Basilisk as "development software" and states "it should be considered more or less beta at all times; it may have some bugs and is provided as-is, with potential defects". It was initially released in November 2017 for Microsoft Windows and Linux.

Epic Privacy Browser

Epic Privacy Browser was released on August 29, 2013 and is developed by Hidden Reflex using the Chromium source code, developed for the security conscious. Epic Privacy Browser is (by default) always in "private browsing mode", taking a proactive approach to ensuring that session data (such as cookies, history, and cache etc.) are removed upon exit. The browser also removes Google tracking and blocks other organisations from tracking users.

Cc Cc Browser

Cc Cc browser is a web browser primarily focused on the Vietnamese market. It is available for Windows and macOS operating systems and supports both the English and Vietnamese languages. It is developed by Vietnamese company Cc Cc and based on the Chromium open source code. Cc Cc is the second most popular browser in Vietnam, with a market share of 16.89%, according to data from StatCounter.

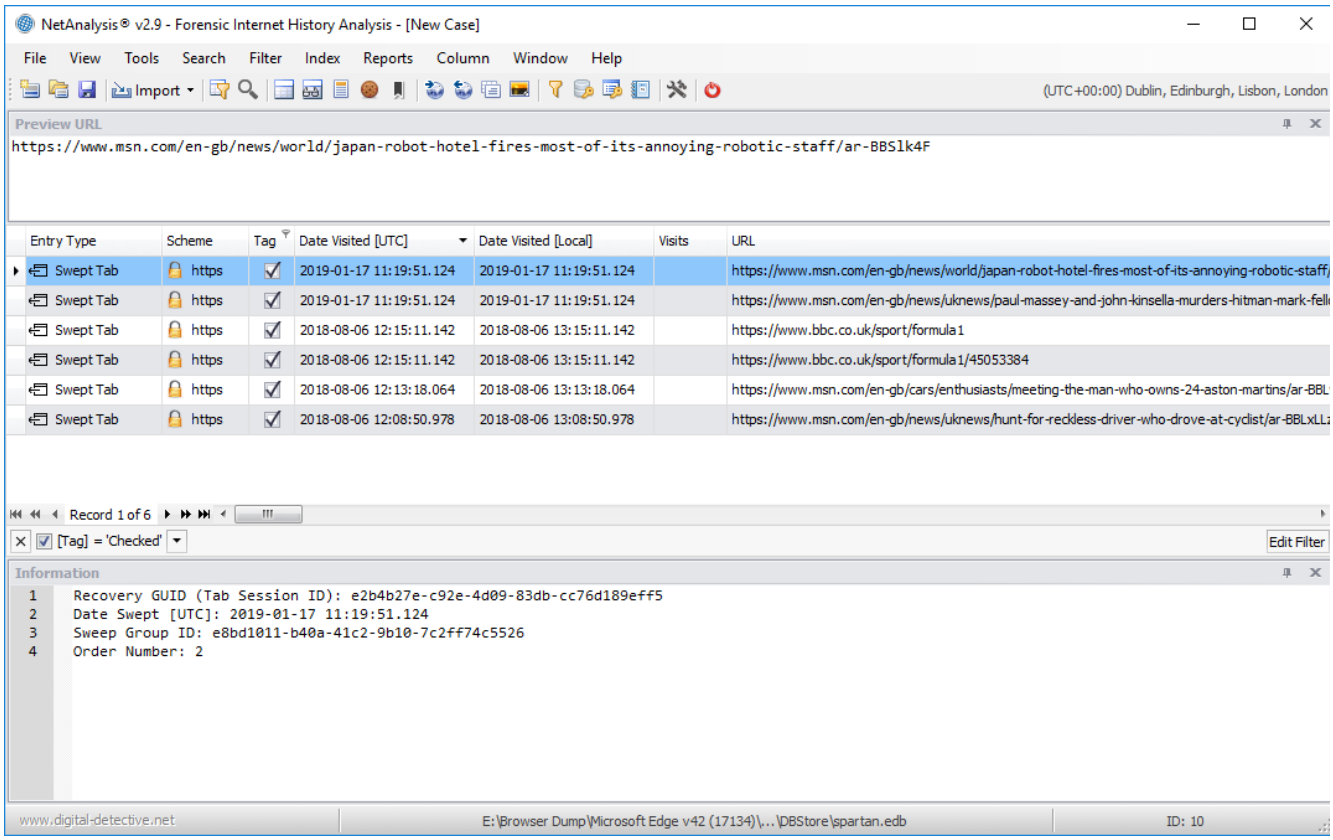
QQ Browser

QQ Browser (QQ) is a Chromium-based web browser for Android, Windows, macOS, and iOS platforms. It is developed by Chinese Internet giant Tencent. The application offers a number of features such as tabbed windows and integration with chat platforms. QQ browser version 9.0 was the first released version which used the Chromium source code (Chromium v43). Prior to this QQ Browser was based on the Trident engine.

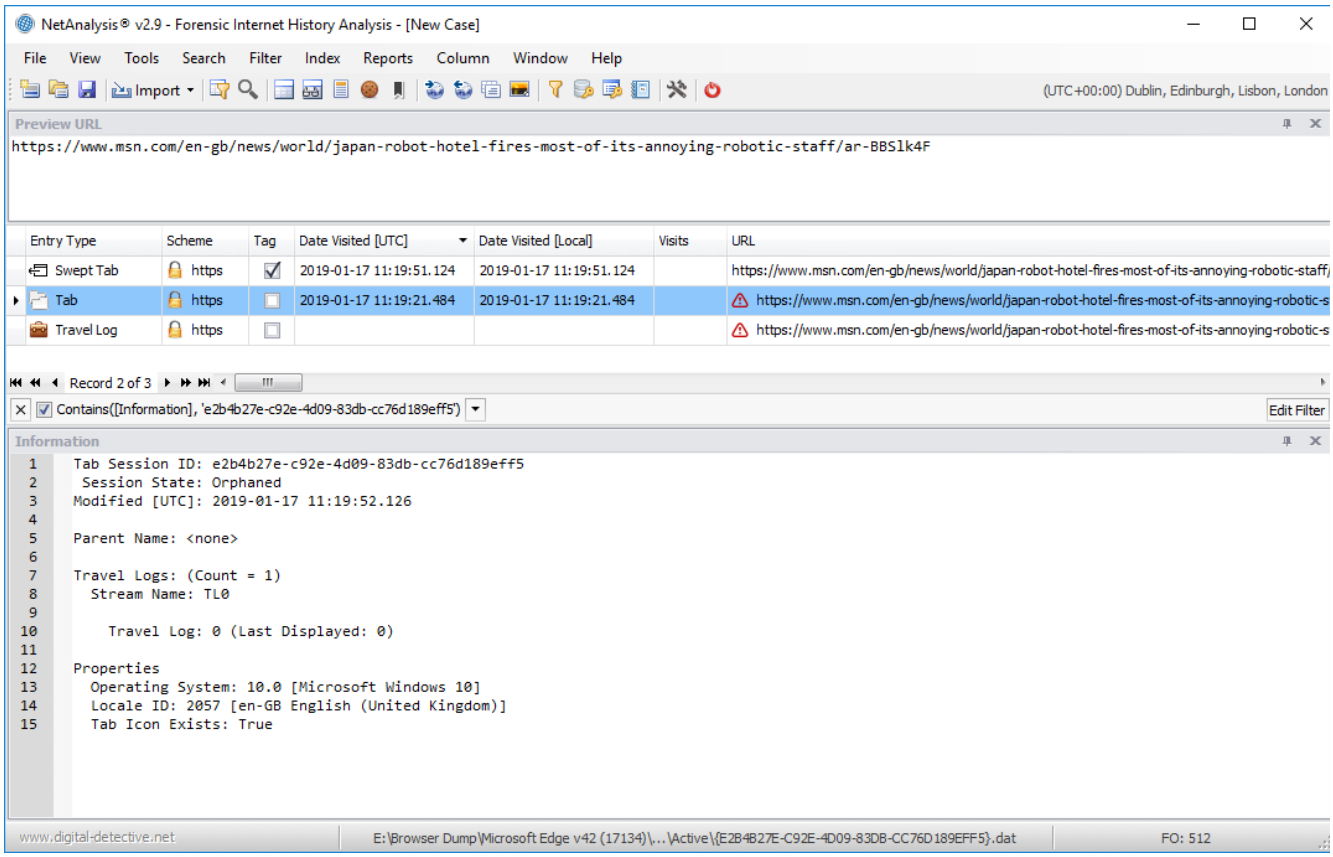
New Support for Existing Browsers

Microsoft Edge Swept Tabs

Microsoft has added a feature to its Edge browser to make it easy to sweep aside all the tabs the user has open into a collection that can be restored at any time. We have now added support to NetAnalysis® for viewing these Swept Tab entries (see below).



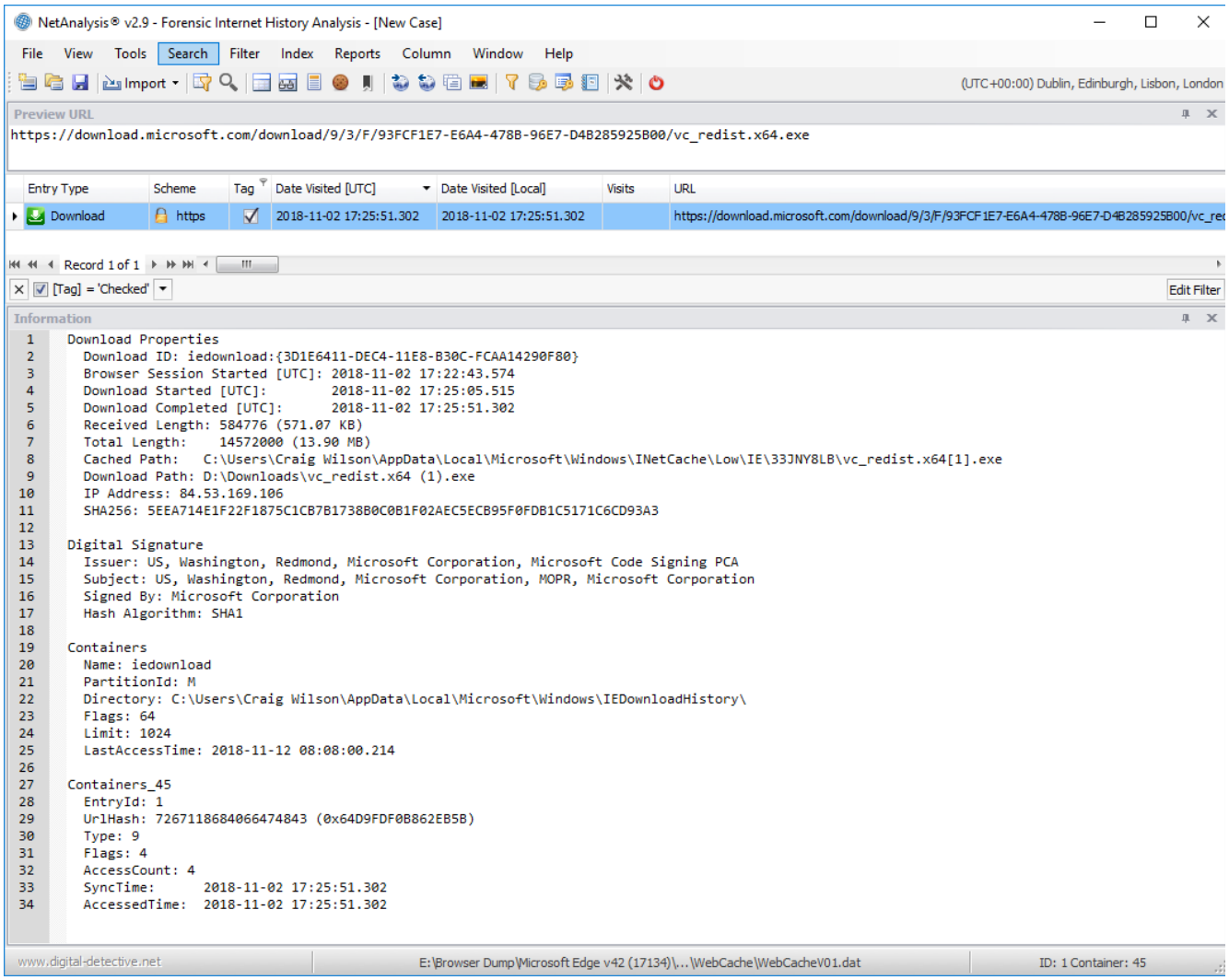
The Recovery GUID shown above is a unique identifier which relates to Recovery Store entries (Tab Session ID). In the screen capture below, you can see we have created a filter looking for records that contain the Swept Tab Recovery GUID in the Information field. This filter returns three records which can be seen below.



Microsoft Edge Downloads

Another area we have improved, in this release, is the processing of the download information object for Microsoft browsers. We have greatly improved the processing of corrupt and partially recovered data through HstEx® and added support for all known versions of the download object (including those versions released in beta and pre-release products).

We have also reformatted the output displayed in the Information panel, to make it clearer and easier to understand (see the screen capture below for an example).



Microsoft Edge Typed URLs

Microsoft Edge v42 changed the location of Typed URLs from the Registry to a table within the spartan.edb database. We have added support for importing Typed URL data from the new location.

Microsoft Edge Cookies

With the release of Microsoft Edge v40, the structure of the table relating to cookie entries completely changed. The older table structure contained information pointing to an externally stored cookie file which was located in the file system. The new cookie table structure brought the actual cookie information into the database table, negating the need to save this information to an external file.

We have added support for importing Cookie data from the new location.

Microsoft Edge HSTS Entries

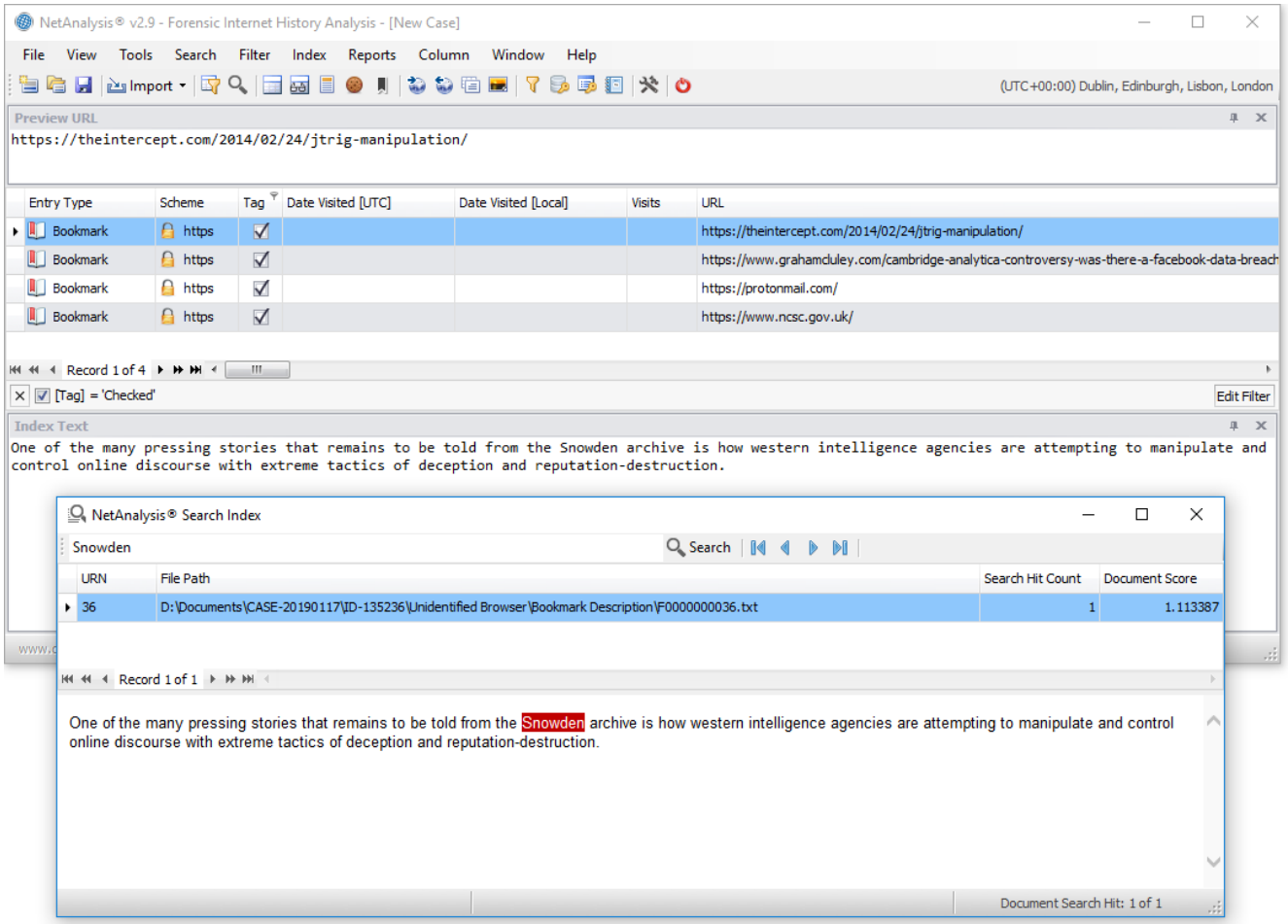
We have added support for the import of data from the HstsEntry tables. This data relates to HTTP Strict Transport Security (HSTS) and is a web security policy mechanism that helps to protect websites against protocol downgrade attacks and cookie hijacking. It allows web servers to declare that web browsers (or other complying user agents) should interact with it using only secure HTTPS connections, and never via the insecure HTTP protocol.

Netscape HTML Bookmark File Description

We have added some additional functionality to our processing of Netscape HTML Bookmark files. If you are unfamiliar with this file type, it is a common format, shared by many browsers, for the import/export of bookmarks and "favorite" entries.

In addition to extracting image and favicon files (which will be displayed in the Viewer panel), we extract the description portion of the entry

so it can be added to the search index. The actual text data can be viewed from the Index panel (as shown below), and can be searched via our Search Index feature.



New Features

Internal HTML Viewer

We have updated our internal viewer so that it supports the latest HTML standards and world wide web technology. We have also added some additional functionality which is accessible from the right-click context menu. The new items are as follows:

- **Save as PDF** - You can now save a rebuilt webpage (or other supported type) to a PDF file.
- **Open Containing Folder** - This will open an Explorer window and will highlight the source file for the content being displayed in the viewer.
- **Open with External Viewer** - This will send the content being displayed in the viewer to the default viewer for your system. For example, if the content relates to a video file, it will send the source to your default video player.
- **Zoom** - The zoom options allow the user to zoom in, out, or reset the zoom level to the content displayed in the viewer.