NetAnalysis v2.10

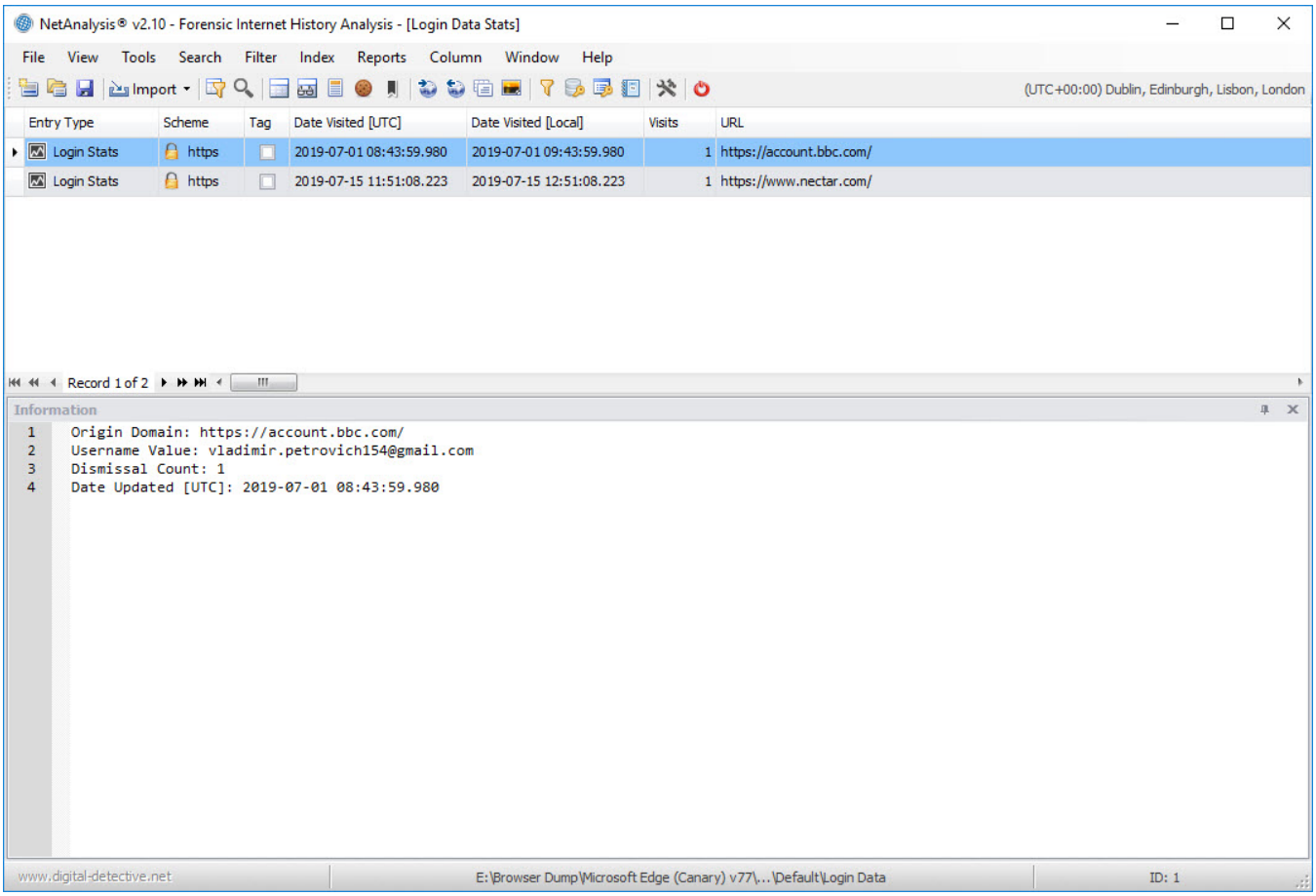
Introduction

This release of NetAnalysis® adds support for the new Microsoft Edge (Chromium) browser, which has been released in Dev and Canary builds; we have also added support for the new Opera GX gaming browser as well as adding support for fifty-eight other browsers.

New Features

Login Stats Entries

We have added support for the recovery of Login Data stats entries for Chromium based browsers. This table records the number of times a user has logged into a password protected domain and dismissed the save password dialogue (for a maximum of three times). Once three instances have been recorded, the browser will no longer offer to save the username/password for the domain.



Microsoft Edge

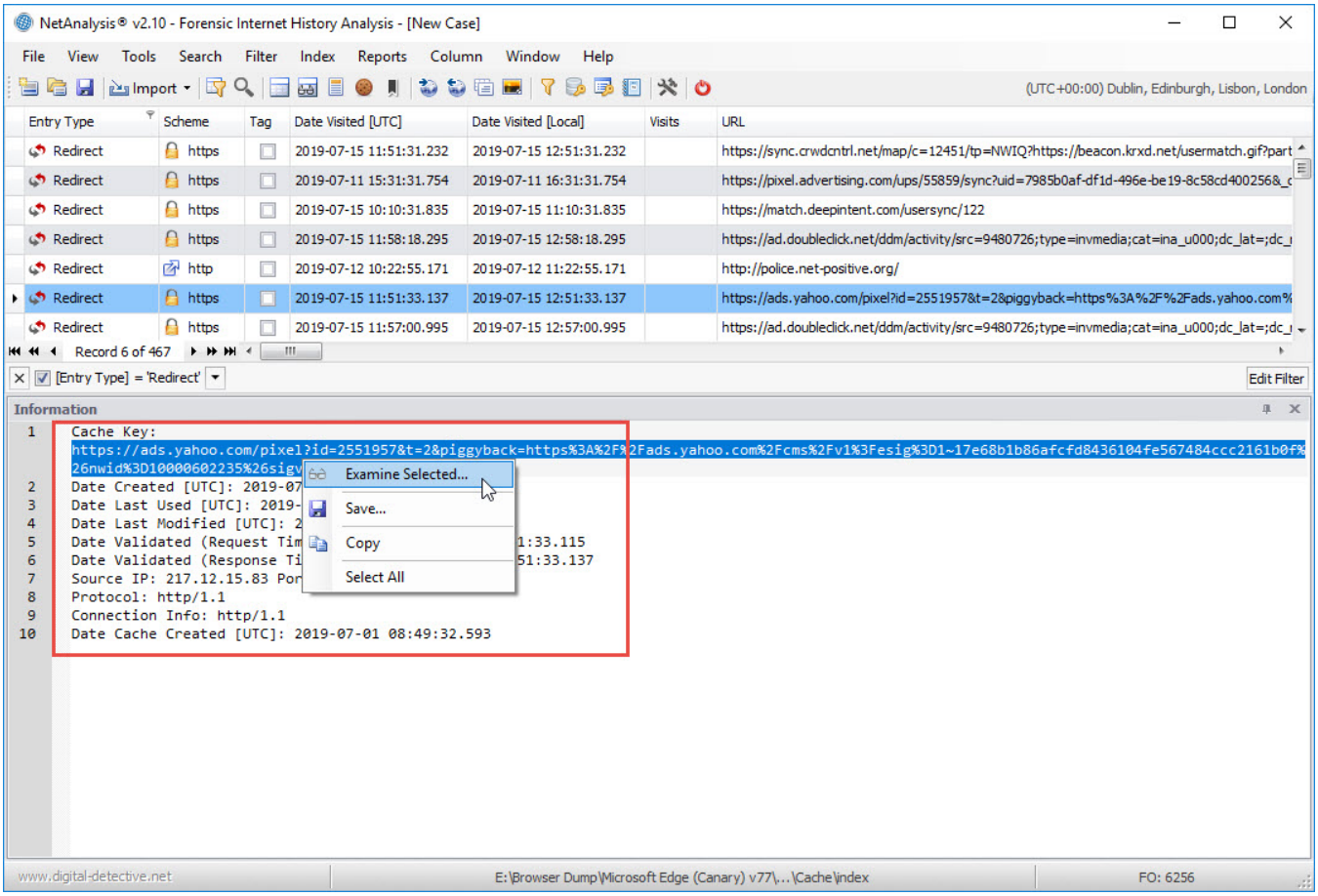
In December 2018, Microsoft announced their intention to adopt the Chromium open source project in the development of their Microsoft Edge browser. As of July 2019, they have released Developer and Canary editions. Microsoft Edge is currently available for Windows 7, 8, 8.1 and 10 as well as supporting macOS.

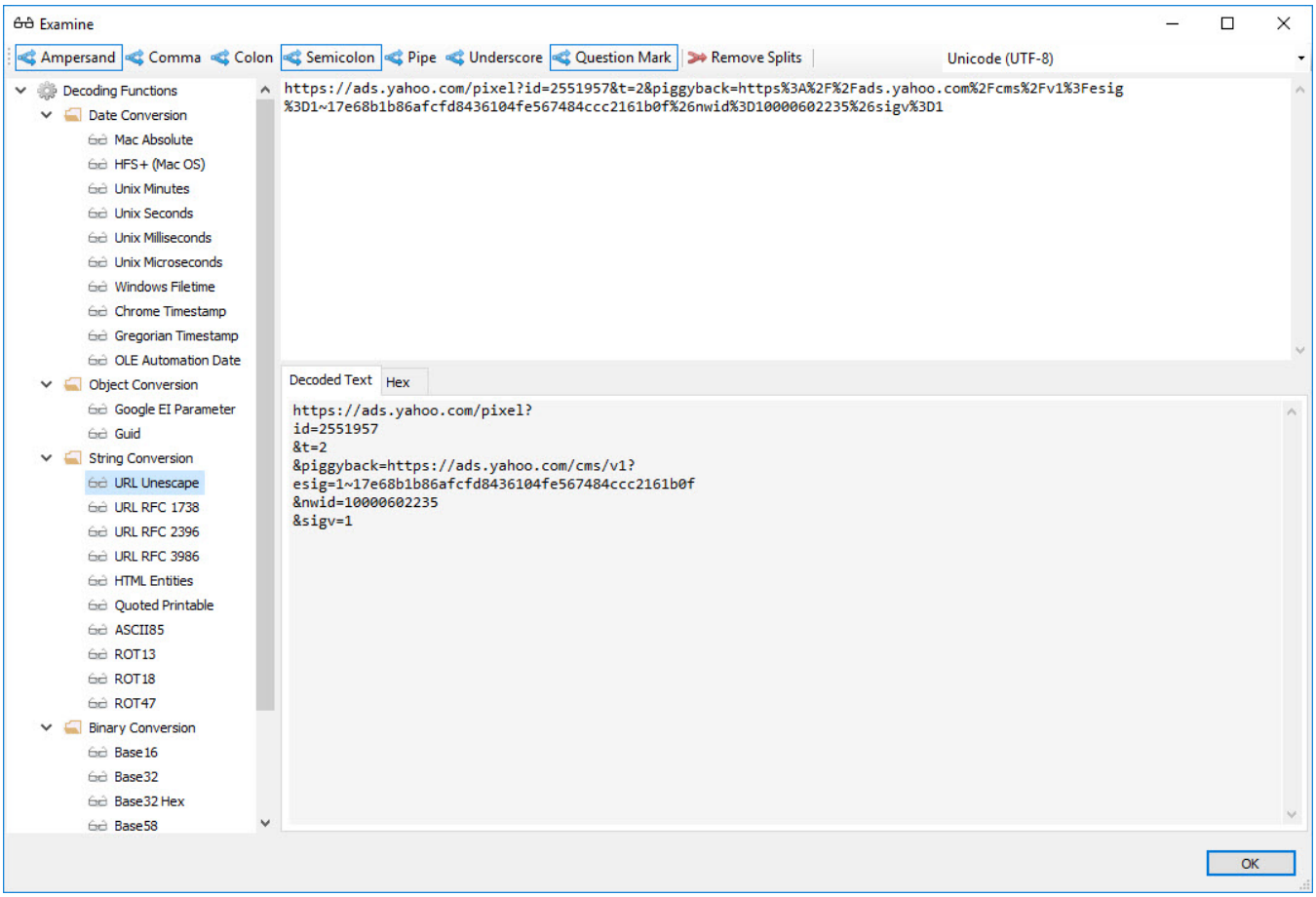
Opera GX

Opera GX is a special version of the Opera browser built specifically to complement gaming. The web browser includes unique features to help the user get the most out of both gaming and browsing. It is a desktop web browser for Windows PCs.

Examine Selected Text

This new feature allows you to select text from the Information panel and send it to the Examination Window for analysis and/or decoding. Simply open the Information panel, select the text you wish to examine, right click and select **Examine Selected**.





New Report Template

We have added a new report template titled "Template with Decoded URL". This can be accessed by opening the **Report Manager** from the **View** menu, or typing **CTRL + Shift + R**. This template demonstrates how to take the Decoded URL data and display it in the split format as displayed in the Decoded URL panel. This is achieved by taking the data from the Decoded URL column, and processing it through a **SplitDecodedUri()** function. The script for the report can be seen by clicking on the **Scripts** tab in the **Report Designer**. The script is shown is the image below.

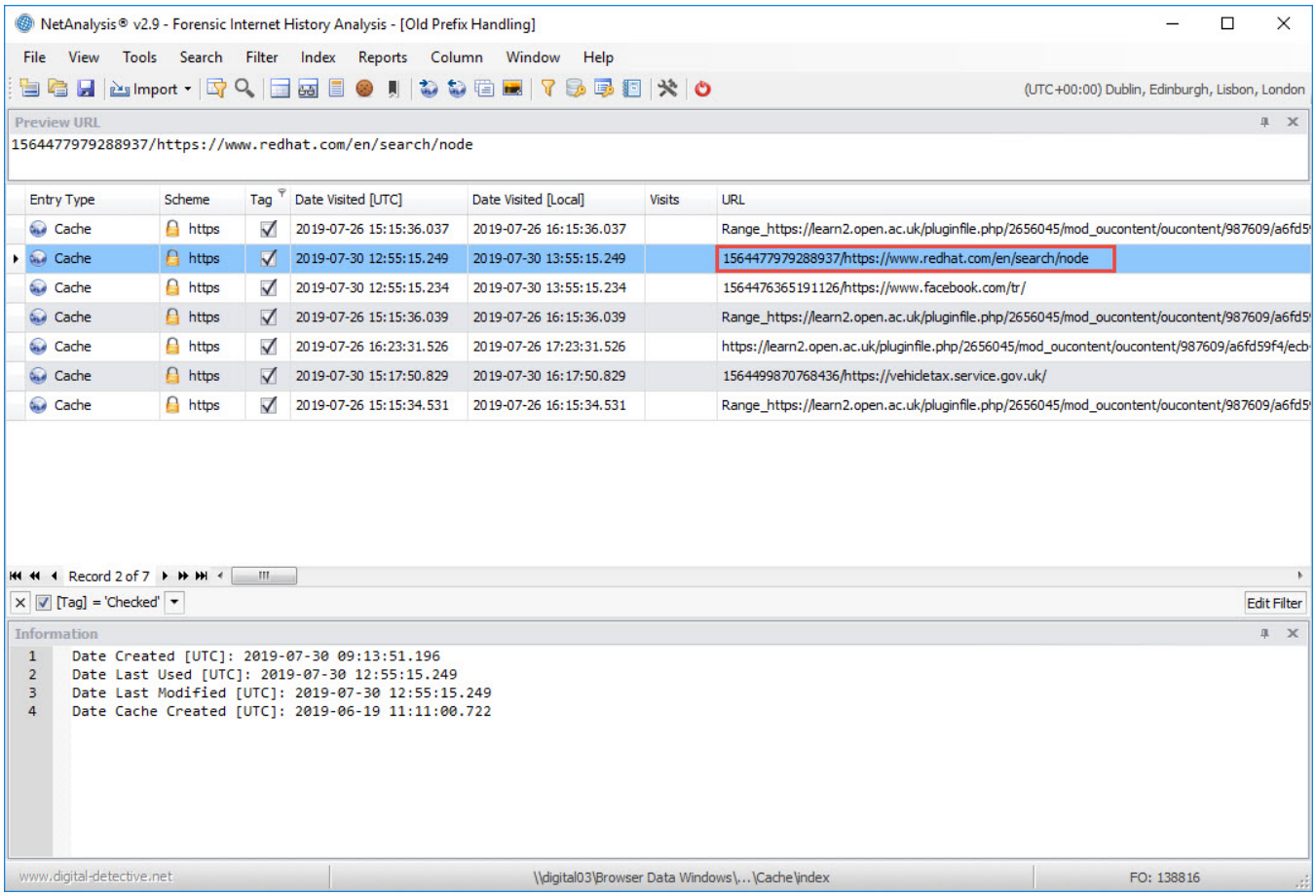
```
13
14  private string SplitDecodedUri(string uriToSplit)
15  {
16      if (string.IsNullOrEmpty(uriToSplit))
17          return (string.Empty);
18
19      uriToSplit = uriToSplit.Replace("?", "?" + Environment.NewLine);
20      uriToSplit = uriToSplit.Replace("&", Environment.NewLine + "&");
21      uriToSplit = uriToSplit.Replace(";", Environment.NewLine + ";");
22
23      return uriToSplit;
24  }
25
26
27  private void ReportDetailedTemplate_DataSourceRowChanged(object sender, DevExpress.XtraReports.UI.DataSourceRowEventArgs e) {
28
29        // Send the decoded URL value through the splitting routine
30        LabelDecodedUrl.Text = SplitDecodedUri((System.String)GetCurrentColumnValue("DecodedURL"));
31
32  }
```

Cache Prefix Handling

The URI key for an entry stored in the cache is normally the URI of the resource (for example ***https://www.digital-detective.net/favicon.ico***).

A cache key may also contain one of more prefix values. These prefixes can be an internal scheme used by the browser when retrieving entries from the cache (Firefox) or indicate a sparse entry where the browser is able to store only parts of a resource (Chrome). The prefixes may contain attribute values used to map the cache entry to a partitioned area of the cache storage (Firefox) or to indicate protocol information stored in the cache (Chrome).

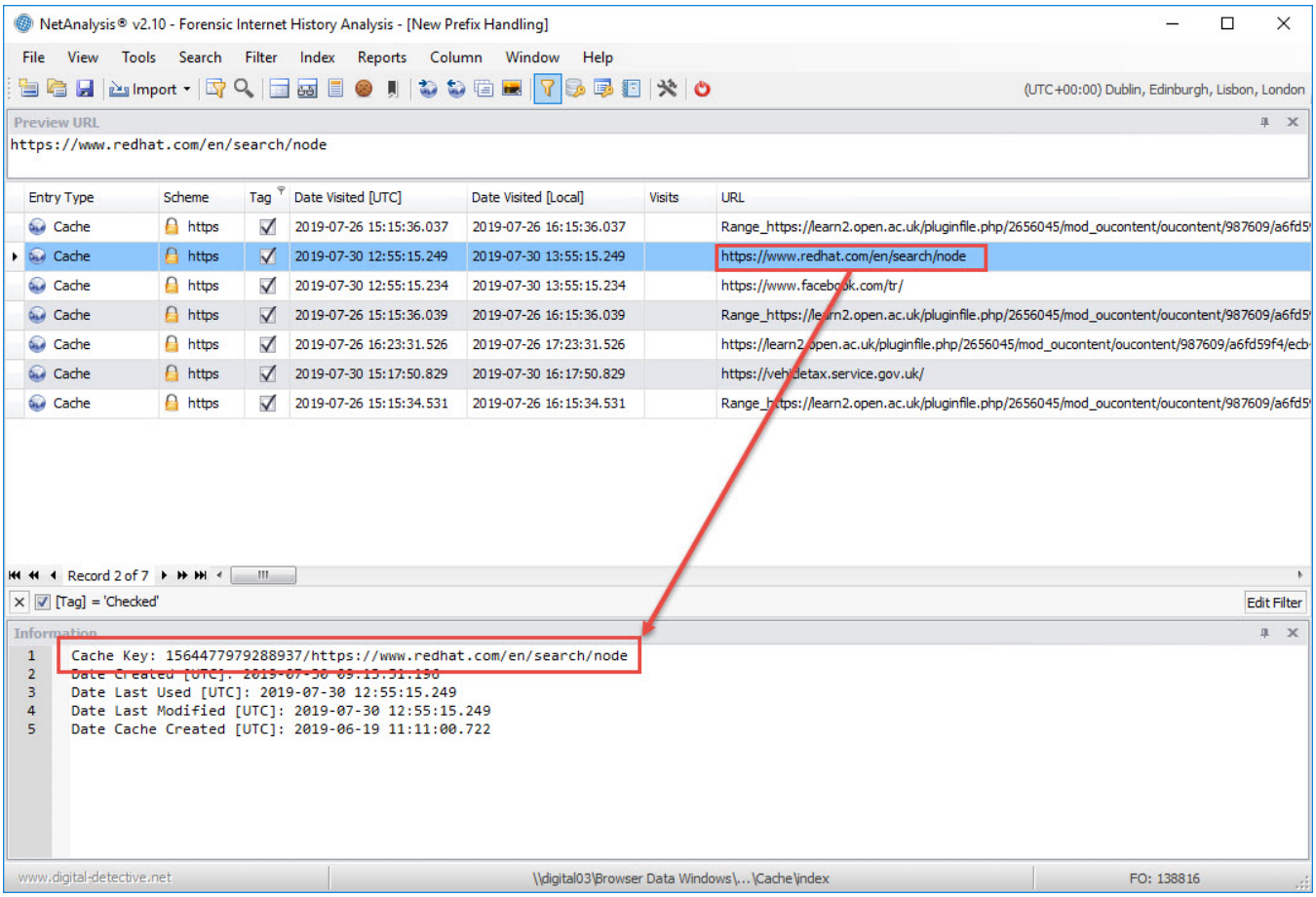
The image below shows a cache entry with prefix as displayed in NetAnalysis® v2.9.



Browsers have now started to include cache key prefixes that indicate cross-origin resource cache entries. The cache keys for these entries actually contain two or more URIs so that the top-level origin can be stored along with the resource URI. This can make cache handling problematic.

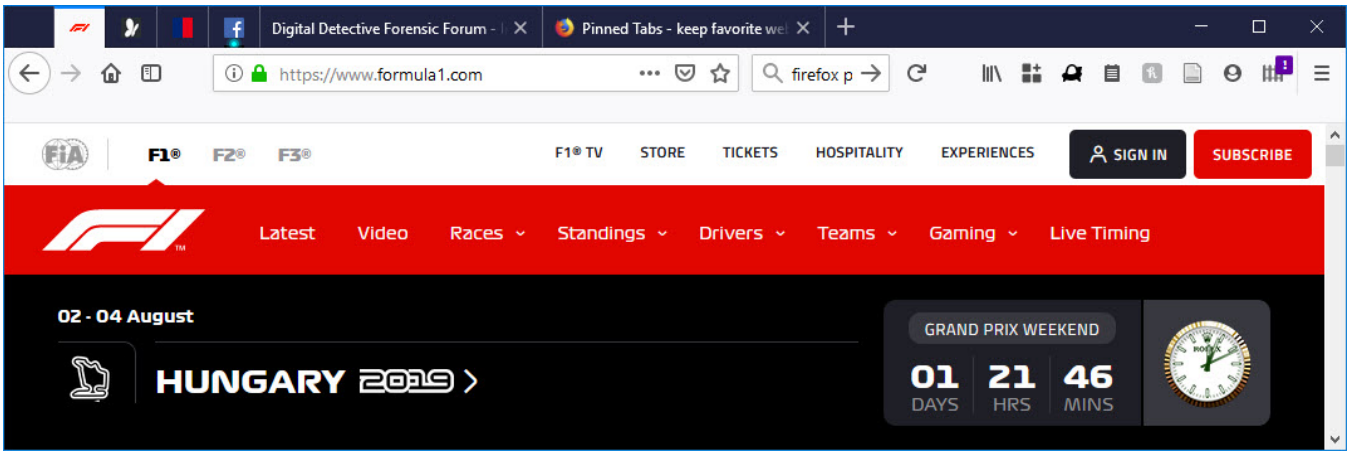
As a result of these changes, we have had to revisit the way NetAnalysis® handles cache entries containing prefixes. From NetAnalysis® v2.10, if a cache entry has a prefix, we will remove this data when handling URLs. This allows for easier URL handling and processing. To retain the original value, we will show this in the Information panel. With the exception of Chrome cache v2 sparse entries, the prefix will be retained to aid with sparse entry identification.

The image below shows a cache entry with prefix as displayed in NetAnalysis® v2.10. The prefix has been removed and the Information Panel shows the original cache key. The sparse entry prefix "Range_" can be seen in the other entries below.

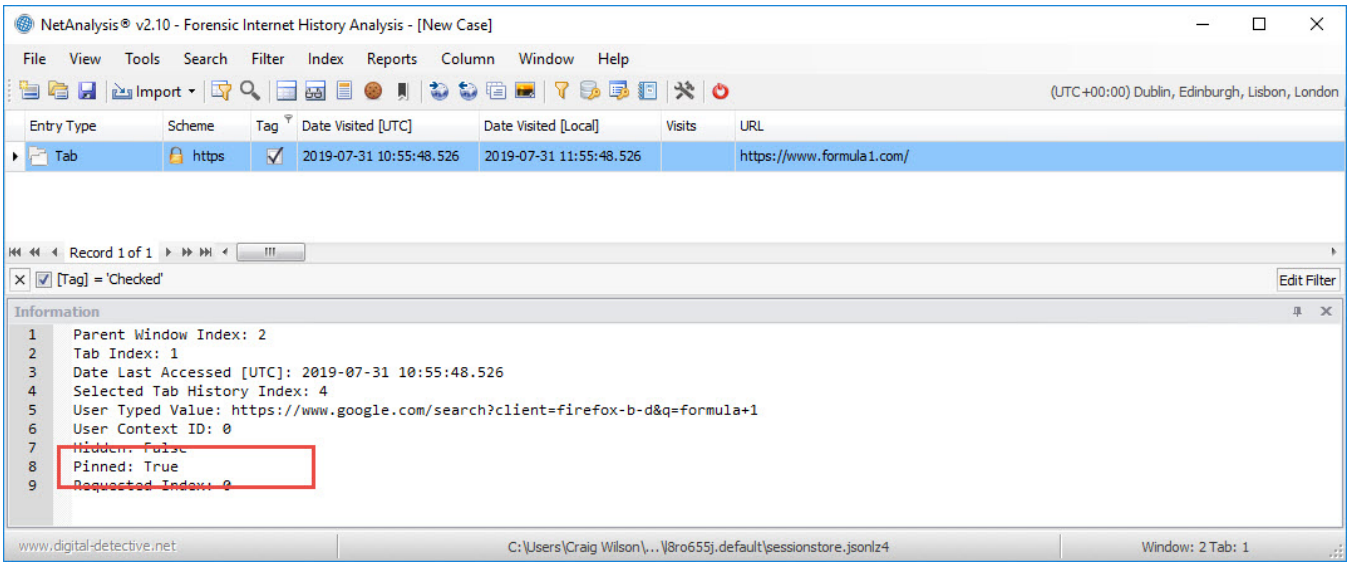


Firefox Pinned Tabs

Firefox recently added a new feature for pinning the tabs of frequently used web sites for easy access. The pinned tabs are small and cannot be closed accidentally, they also open automatically when the browser is restarted. The user can easily pin a tab by right clicking on any tab and selecting Pin Tab from the menu (see the image below for Firefox pinned tabs, shown to the top left of this browser).

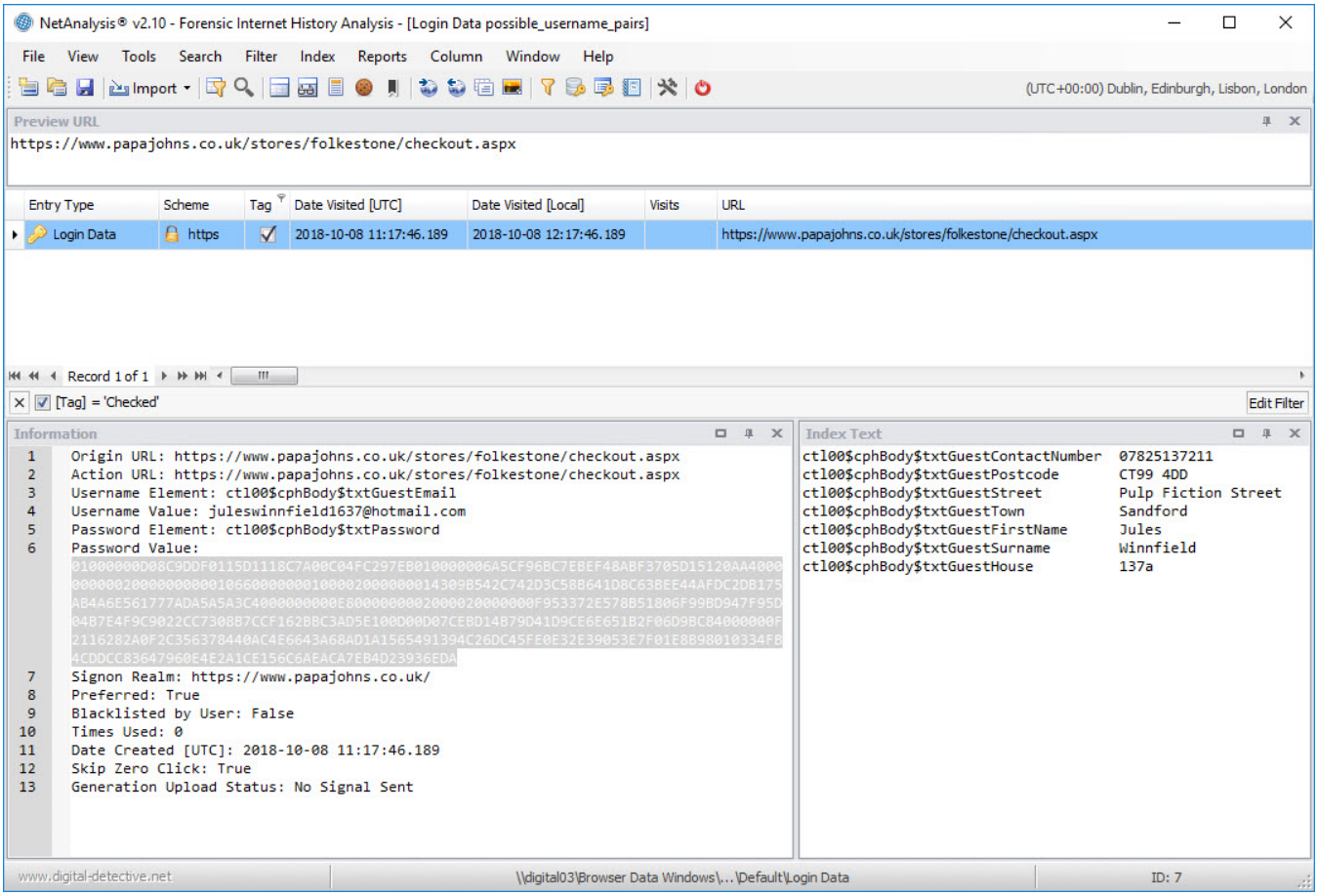


To identify a pinned tab, open the sessionstore file in NetAnalysis® and review the Information window as shown below.



Chromium Login Data Name/Value Pairs

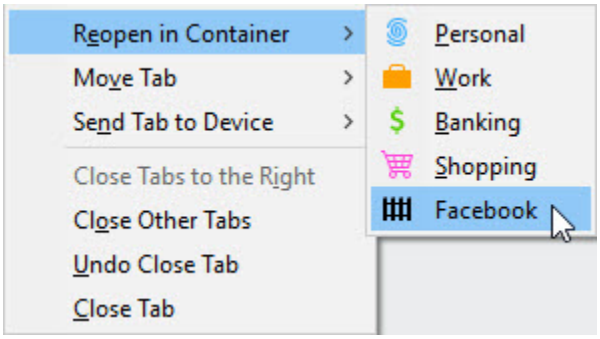
We have enhanced the handling of Chromium based login data in NetAnalysis® v2.10. The name/value pairs are now extracted and displayed in the **Index Text** window. The data is also written to the export folder so that the information can be indexed by our search engine. In the example below, our user has logged in to the web site of a local pizza company so that some tasty food can be ordered (and delivered). The **Index Text** window in this case shows the user's name, contact number and delivery address. The **Information** window shows other information relevant to this transaction.



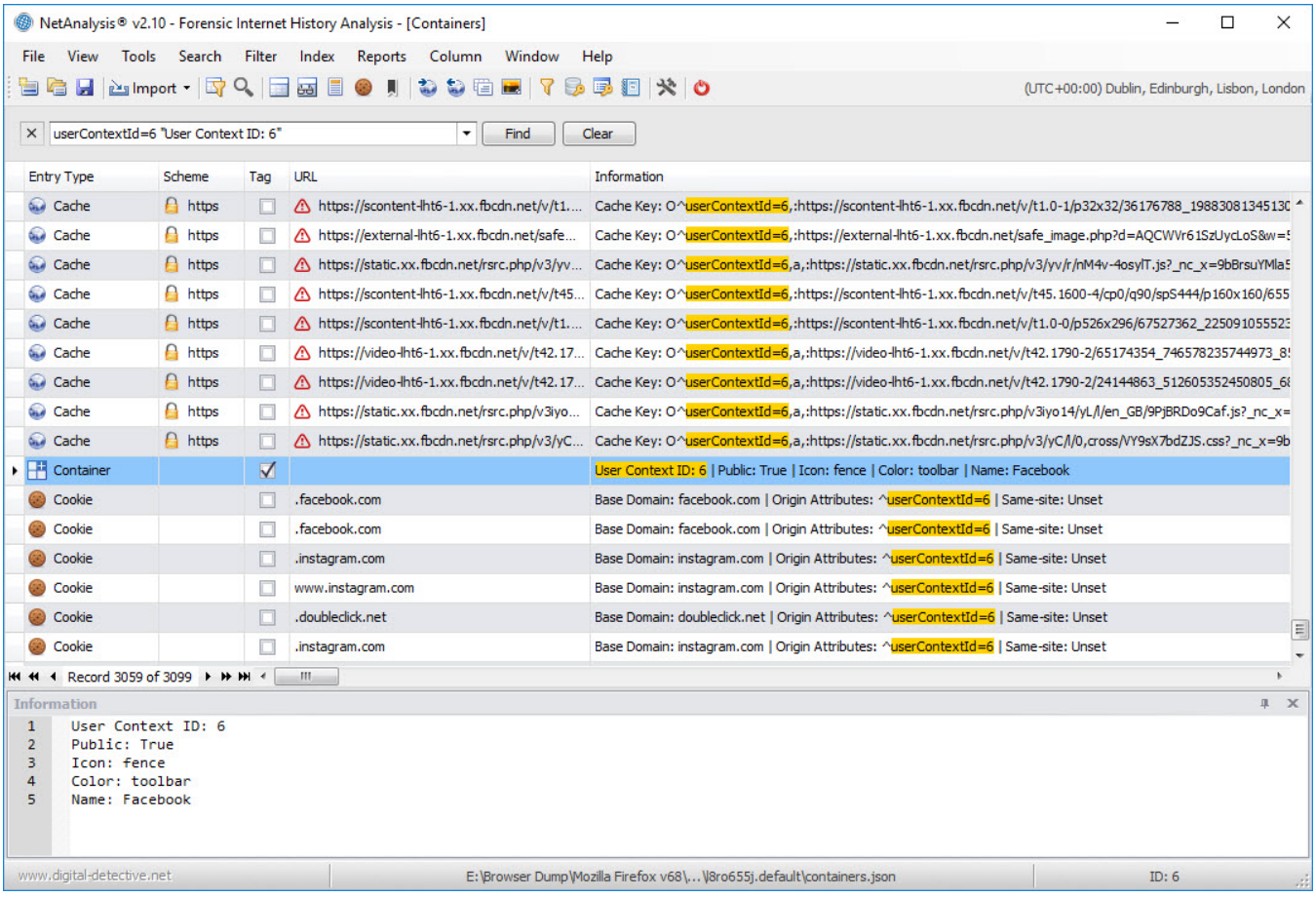
Mozilla Firefox Containers

The Firefox Multi-Account Containers extension lets the user create a separate box for each of their online lives; which means they don't have to open a different browser to separate work and home browsing. The extension separates website storage into tab-specific Containers. Cookies downloaded by one Container are not available to other Containers, so the user can log into the same site with different accounts and online trackers can't easily connect the browsing. Custom labels and colour-coded tabs help keep the different activities or personas separate.

Existing tabs can be re-opened in a specific container by selecting from a right-click menu (see below).



NetAnalysis® 2.10 now supports the import of data from Firefox Multi-Account Containers. The image below shows a container entry, and the Information window shows the corresponding unique user context ID. This value identifies the Container. In this case, we are looking at the Facebook container. This ID can then be used to identify other entries and activity related to that container.



Change Log

To review the full list of changes for this release, please see: Change Log v2.10.