HstEx v4.8

Introduction

The major new feature for this release is the ability to process logical evidence files (L01/Lx01) as a source. We have also added support for two new browsers as well as adding new artefacts to the existing browser support.

New Features

We have added new support for HstEx® v4.8 to recover the following:

Chromium Shortcut Entries

Many of the Chromium based browsers have an Omnibox feature. An Omnibox is similar to the traditional web browser address bar, but the user can also use it like a search engine. The purpose of Chromium's Omnibox is to merge both location and search fields while offering the user some highly relevant suggestions and/or early results. The aim of the Omnibox is to provide tools that allow the user to reach their destination page faster. The Shortcuts database contains information which links the text entered into the Omnibox with the selected address.

With HstEx® v4.8, we have added the ability to recover individual Shortcut entries so they may be imported into NetAnalysis®. They can be selected as follows:

Mozilla Permission Entries

Many of the Mozilla based browsers have a Permissions Manager that provides the user the ability to configure a number of site-specific

settings for an individual website. These options include whether or not to store passwords, share location with the server, set cookies, open pop-up windows, or maintain offline storage. Rather than configuring these privacy and security options for all sites, the Permissions Manager allows the user to define different rules for different sites.

With HstEx® v4.8, we have added the ability to recover individual Permission entries so they may be imported into NetAnalysis®. They can be selected as follows:

Microsoft Edge Favorite Entries

Microsoft Edge v25 saw some changes to the way the browser stored user data. The favorite entries moved to an ESE database called spartan.edb. With HstEx® v4.8, we have added the ability to recover individual 'Favorite' entries so they may be imported into NetAnalysis®. They can be selected as follows:

Support for Processing Logical Evidence Files

EnCase® Logical evidence files (.L01 and .Lx01) are created from previews, existing evidence files, or Smartphone acquisitions. These are typically created during an analysis when specific files of interest are identified. These files can then be extracted to a separate evidence container.

HstEx® v4.8 now has the ability to read and process .L01 and .Lx01 image files.

New Browser Support

We have added new 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 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.

HstEx® v4.8 can recover the following artefacts:

Improvements

We are constantly updating and improving our profiles for more accurate and faster recovery. In this release, we have updated the following recovery profiles:

- Mozilla Firefox Cookie entry recovery.
- Google Chrome Cookie entry recovery.
- Google Chrome History entry recovery.

Change Log

To review the full list of changes for this release, please see: Change Log v4.8.