Intella 2.3 Release Notes

Highlights

- Introducing a new product: **W4**, for the rapid analysis of user activity.
- Added support for **load file overlays**.
- Items can now be exported to an **item report**.
- Added support for MS Exchange **EDB 2013/2016** files.
- Added support for **Outlook for Mac** olk15* files.
- Added a user interface for managing **memory and crawling settings**.

W4

The Intella 2.3 release coincides with the launch of a new Vound product: W4.

W4 is an application for detecting user activity in a disk image or file collection. With W4, you can quickly answer questions such as:

- Does the user possess material of type X (e.g. documents, images, emails, chat messages, notable application types) and what do these items look like?
- What USB devices were used; what files have been copied to those devices?
- What web pages were visited and what files were downloaded?
- What files were sent or received by email?
- What programs were launched?
- What folders were explored?
- Is this evidence data relevant to my investigation, and what follow-up analysis is warranted?

Key benefits of W4 are:

- **Easy to use interface**; the very gentle learning curve makes it suitable for non-specialists.
- **Very fast indexing** allows to quickly scan and assess the evidence.
- **Search during indexing** lets one see the first results within minutes.
- A **powerful indexing engine** supporting a variety of system and registry artifacts.
- A **Timeline** for visualizing data distribution over time and filtering items.
- The innovative **Events** view allows for seeing all user actions in a single unified chart. Events can be annotated via tags and notes, allowing for the creation of a custom timeline.
- A **Thumbnails** view for easy previewing of all images in the case.
- Simple to use **annotation tools**, for tagging items and adding notes.
- The **Item Links** feature allows unveiling and exploring hidden links between artifacts, such as documents copied to a USB device, downloaded from the Internet, or sent by email.
- Flexible **reporting** functionality, with sections that can be configured individually (table, events, image gallery or link graph), to create professionally styled reports.

W4 and Intella are separate yet complementary applications. A smooth transition path is possible, where data is first investigated in W4 and then further analyzed in Intella. The more extensive indexing, analysis and exporting functionalities that Intella has to offer can then be used on the case.

W4 cases can be added via Intella's Add New Source wizard. When W4 detects an Intella 2.3 installation, it will also show a "Process in Intella" button in its Case Manager.

When adding the W4 source in Intella, the investigator can select what case elements should be carried across. For example, tags, item notes and keyword lists can be either copied into or left out of the Intella case.

Intella can also enhance the W4 case data. It can analyze the items that were already tagged in the W4 case and suggest additional, similarly looking items that come to light through Intella's deeper indexing of the evidence data. Furthermore, item data can be enhanced during the import phase through content analysis, OCR, or by re-applying keyword lists.

Once the source has been imported, a top-level tab is added to Intella, showing how the original W4 case has been expanded. The number of additional items that were found are listed, grouped by file category and type. Newly tagged items, through tag analysis and keyword lists, are reported.

To learn more about W4, please visit https://www.vound-software.com/W4.

Installer

- Resolved an issue with the Browse button in the installer not functioning properly.

Indexing

- The memory settings and maximum crawler count for the indexing engine can now be managed from within the user interface. Before, this was controlled via the l4j.ini files in the application folder. The settings are now case-specific rather than installation-specific.
- Added support for MS Exchange EDB 2013 and 2016 files.
- Added support for Outlook for Mac olk15* files.
- Added support for Apple Disk Image (DMG) files. Please see the User Manual for which compression methods are supported.
- Added support for indexing installed and startup programs found in the Windows registry.
- Added support for indexing UserAssist entries, prefetch files and jump lists.
- Added support for LNK and URL files. Previously these could only be identified.
- Added support for Windows XML event log (.evtx) files, including logon and logoff events.
- Added support for extracting artifacts from Windows.old folders, which may be present after a major Windows update has been performed.
- Improved support for indexing the contents of Recycle Bins, including metadata such as time of deletion.
- Updated the Office 365 and SharePoint connectors in accordance with changes to these Microsoft services. Furthermore, these connectors have been made more robust against server errors.
- Updated the iCloud connector in accordance with changes to this Apple service.
- Preserved text styling when extracting the contents of an RTF-encoded PST/MSG/EDB email.
- Improved the extraction of non-Latin and/or long file names in MIME-formatted emails.
- Improved calculation of message hashes of items whose attachments are organized in a folder tree.

- Resolved an issue with non-matching paragraph hashes due to the line breaks that are introduced by certain email clients.
- Resolved an issue with the parsing of LDAP email addresses that lack a domain.
- Resolved an issue with SMS messages in Cellebrite reports being incorrectly classified as "Unsent".
- Made the parsing of Skype databases more robust.
- Resolved an issue with the incorrect modeling of the hierarchy of the root item in an L01 image, which could trigger a variety of problems.
- Resolved an issue with certain PST calendar items missing a location property.
- Resolved issues with the indexing of MS Internet Explorer 10, 11 and Edge web history on Windows 10.
- Resolved an issue with items from MS Outlook for Mac OLM files missing a location property.

Indexing - Load Files

- Added support for adding a load file overlay. This lets one extend or overwrite the metadata of previously imported load file items.
- Resolved an issue with load files in UTF-8 format that start with a Byte Order Mark (BOM). The BOM would become part of the first column name.
- Resolved an issue with tag columns with multiple values not being parsed correctly, resulting in the tags being reported as a single concatenated tag.

OCR

- Updated the embedded OCR engine. This fixes several issues with problematic PDFs.
- Resolved an issue with the CSV file holding the OCR log not being written properly.

Searching

- A Statistics dialog has been added to the Details view's popup menu. This dialog lists statistics about the selected items, such as their cumulative file size, total number of document pages, as well as other attributes.
- Added a separate keyword search option for file names, so that they can be searched independently from their folder names.
- IBM Sametime chat dumps are now listed in the Type facet beneath Chat Conversations, rather than Forensic Containers.
- Resolved the incorrect determination of top-level items in SharePoint and Office 365 sources.
- Resolved an issue with incorrect results of phrase queries with wildcards on items with reviewer comments.

Keywords Tab

- Resolved an issue where searching using keyword lists in the Keywords tab where imported texts (e.g. using the -importText command line argument) were not included.
- Resolved an issue with incorrect item counts for certain types of Boolean queries and with the "Hits" option selected in the Calculate section.
- Resolved an issue with incorrect hit counts on certain types of complex phrase queries.

Tasks

- Added an option to select all items in a task.

Social Graph

- Added a Review menu option to the Social Graph's popup menu.

Previewer

- Various improvements to the rendering of PDF documents containing charts.
- Improved the rendering of chat conversation items that lack sender information.
- The Words tab is now always shown; it is no longer tied to the presence of the Contents tab.
- The visit date of typed URLs is now being shown in the Previewer.

Redaction

- Resolved an issue with keyword search in the Redaction tab not working properly due to the incorrect handling of whitespace characters between words in the item text.

TEAM

- Resolved an issue with the communication with remote cases not being restored properly after a temporary network glitch.

Exporting - General

- Added exporting of selected items to an item report. Such a report lists a user-defined set of content and metadata properties of the selected items, in a table, list or thumbnail gallery. Various options for sorting, styling, and other customization of the report are available. Item reports can be exported to PDF and DOCX format.
  An item report should not be confused with an export report. The purpose of an export report is to log what items were exported to e.g. PDF, PST or native format, including any errors that occurred during that process.
- Resolved an issue with the Default button in the Export wizard's export template section not always working correctly.

Exporting – PDF

- Optimized performance by reducing the number of child processes that is generated during the generation of the PDFs.

Exporting – Load Files

- When an item has redactions applied to it, one can now suppress the exporting of the natives of all items in the item family. Before, only the natives of the redacted items themselves could be suppressed. This could lead to the redacted content still being exported in unredacted form when a family member was exported.
- Added an ATTACH_RANGE field, which combines the RECORD_ID_GROUP_BEGIN and RECORD_ID_GROUP_END values in a single exportable field.
- Resolved an issue with the generated HTML structure of emails whose body was originally encapsulated in RTF format in a PST/MSG/EDB email. The generated HTML would render correctly in email clients but did not render well in Relativity.

- Resolved an issue with the exporting of chat conversation items to a load file. If the conversation item has attachments, the exported extracted text of the chat item would contain references to those attachments. These references are now suppressed.
- Resolved an issue with newly created export sets not being available in the advanced file naming column chooser until after Intella had been restarted.

Upgrade Notes

A dongle update is needed to upgrade from earlier Intella versions.

Intella 2.3 can directly open cases made with Intella 2.2.x and 2.1.x.

When a case made with Intella 2.1 or older is opened, all Content Analysis results are automatically migrated to a new data storage format. This migration happens only once. The old store is retained and will still be used when using version 2.1 or older. New results will not be added to the old store though, and new results added to the old store will not be migrated. Cases made with 2.1.1 or later already use the new data store and are therefore not affected.

When items in cases made with 2.1.x are exported to a separate case, the registered case size of the target case will be incremented with the size of the original case. This may be problematic for users with licenses that have a case size limitation. To resolve the inflated case size, the source case needs to be re-indexed before exporting items from it.

In Intella 2.2.2, a new method for calculating message hashes was introduced. While this change is transparent, please be aware that message hashes will change when re-indexing a case that has been made with an older Intella version.

Intella 2.3 can open cases made with Intella 1.9.x and 2.0.x, but these cases first require conversion before they can be opened. Case conversion will create a copy of the case in which all item data is converted, and all tags, comments and flags are imported. The existing case will not be altered in any way and can afterwards still be opened in the older Intella version. Access to the original evidence files is not required for case conversion.

Case conversion will not transfer the geolocation metadata extracted from emails when the "Determine geographic location of emails" option was used. Re-indexing of the converted case is required to restore such metadata.

Case conversion will require sufficient disk space. As a rule of thumb, please reserve twice the amount of the evidence size for your case folder.

Cases made with Intella 1.8.x or older are not supported.

Cases made with beta versions are not supported and should be recreated.