Intella 2.3.1 Release Notes

Released: **December 20, 2019.**

Highlights

- Index **BitLocker** disk images, **APFS** file systems and Slack exported content.
- Added **hash-based filtering** of items during indexing, e.g. for **deNISTing**.
- Added a top-level **Errors tab**, giving an overview of all indexing errors.
- Added **colored tags**.

- Improved **Includes** functionality.
- Several improvements to the **Keywords tab**, including new export options.
- Added **redaction templates** and **text overlays**.
- Added **Custom ID** and **Custom Family ID** columns.

Indexing

- Added support for BitLocker-encrypted disk images.
- Added support for disk images containing APFS file systems. APFS-level file encryption is supported. Volume-level encryption, e.g. encrypted DMG images, are not supported.
- Added support for indexing exported Slack content.
- Added support for filtering files during indexing based on a repository of known hashes. This can be used for deNISTing items, among other tasks.
- Added support for indexing Skype 14.x databases.
- Added type detection for HEIF/HEIC image files.
- Added metadata extraction for HEIF image files.
- Added detection of MacOS encrypted disk images.
- Added detection of AMR audio files. These are often used to record voicemails.
- Added an Errors tab that opens at the end of indexing.
- Added support for extracting launched programs from the Background Activity Monitor (BAM) Cache in Windows 10 disk images.
- Added support for extracting launched programs and recently used files from the RecentApps registry key in Windows 10 disk images.
- Added support for extracting the Windows 10 build number and release ID.

- Added support for Volume serial numbers in LNK files and jump lists.
- Added support for extracting "Target ID List" properties from LNK files and jump lists.
- Performance optimizations of the post-crawling indexing phases. The optimizations are especially significant when using network shares.
- Improved indexing of MS Office and RTF documents.
- Improved indexing of MS Exchange databases.
- Improved indexing of Cellebrite UFDR reports.
- Improved indexing of Oxygen XML reports.
- Improved indexing of Skype 7.x databases.
- Improved indexing of Dropbox for Business accounts.
- Improved error reporting when indexing Windows 10 Mail containers.
- Improved extraction output and memory usage of PDF document processing.
- Improved processing of VCards.
- Improved processing of Outlook for Mac olk15* files.
- Resolved an issue with certain disk images not being processed when they are contained in an archive.
- Resolved an issue with the list of users in a Dropbox source not listing all users.

- Resolved network protocol errors when connecting to an iCloud account.
- Resolved an issue with the timestamps in EXIF metadata being interpreted incorrectly.
- Resolved an issue with the MD5 of contact and calendar items changing during re-indexing of a case.
- Resolved an issue with SMS messages in Oxygen XML reports not being decoded properly.
- Resolved an issue with documents whose language could not be determined being mistakenly classified as "Not applicable" rather than "Unidentified".
- Resolved an issue where the ffmpeg and exiftool commandline tools were inadvertently being launched during indexing.
- Resolved an issue with the indexing of Windows Event Log .etvx files not working correctly when the case folder was accessed via a UNC path.
- Resolved an issue with very high memory usage when processing certain XML documents.
- Added support for IBM Notes 10 and verified that NSF files can successfully be indexed with an IBM Notes 10 installation. In our tests, the MD5s were different for a small amount of the items (< 1%), compared to when older Notes versions are used. Sampling these items showed that this is typically due to small changes in formatting that had no impact on the conceptual content of the item.
- Added safeguards against noisy data ending up in the keyword index.
- Custom columns can now be case-insensitive.
- Improved the wording in the Check Folder Size and Case Size Limit Exceeded dialogs. These dialogs may show when using an Intella license with a maximum case size restriction or when attempting to index an evidence set larger than the allowed size.
- Stability improvements and updates required for the Office 365 and SharePoint connectors.

Indexing – Load Files

- Usability improvements when importing Tag Groups.
- Resolved an issue with the Conversation Index column getting filled with zeroes upon certain load file imports.

Tasks

- Added the ability to define Custom IDs. These IDs reflect the item location/family structure and can be used to identify items within their families during review.
- Added the ability to define Custom Family IDs. These are either equal to the top-level parent's Custom ID or are derived from the range of Custom IDs that occur in an item family. Family IDs can be used for sorting purposes.

OCR

- Resolved an issue with OCR failing due to a lack of write permissions in certain locations.

Insight

- Optimized calculation of the table holding the top 10 email addresses.

Analysis

- Reduced memory consumption of the email threading calculations.

Searching

- The "Includes" functionality has been renamed, "Required". When adding two or more item sets to the Required list, a drop-down will appear that lets the reviewer choose whether items passing this filter should be in any or all the item sets. Previously, the Includes functionality required that an item was present in any of the item sets. This approach did not work for all use cases.
- Added a "Downloaded from Internet" category in the Features facet.
- Performance optimizations targeting a specific case database that gave issues when the case contained more than approximately 107 million items.
- Resolved an issue with the "Export Sets" facet not highlighting facet values.
- Resolved an issue with the 'Smart Search' dialog not enabling certain document fields for certain item types.
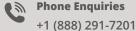
Social Graph

- Resolved an error that occurred when using the mouse wheel to zoom in an empty social graph.

Results

- Added Custom ID and Custom Family ID columns. See the Tasks section for more details.
- Added a Phone Call Type column, indicating the type or direction of a phone call.
- Added a Queued for Redaction column.
- Resolved an issue with the table scrolling back to the start when columns were resized.

Previewer

- MSG emails can now be previewed in their native layout.
- Chat conversation items now show seconds in the timestamps of the individual messages.
- The dialogs that open when choosing the Print option in the right-click menu can now be cancelled.
- Resolved an issue with the Quick Tags panel not updating properly when tags are deleted from the Tags facet.
- Resolved an issue with incorrect word frequencies in the Words tab.

Keywords tab

- A "Totals" line has been added at the bottom of the table.

- An "Exclusive items" column has been added. For each query, this column shows the number of items that are returned by that query and by none of the other queries in the keyword list.

- The entire table can now be filtered by one or more saved searches. This lets one evaluate a keyword list on a subset of the case, e.g. a specific custodian or date range. Previously, saved searches were added as additional columns in the table. While this would calculate the intersection of each query with that saved search, this would not calculate the deduplicated items and family items within the filtered set.

- The table can now be exported to a report in PDF or DOCX format. Several charts are shown that provide additional insight into the keyword list's results.

- The table can now also be exported as an Excel XLSX spreadsheet. This has several benefits over the already existing export to CSV in how it handles characters other than plain ASCII.

- Resolved an issue with the querying functionality not querying for the correct term when the table was not sorted in the default order.

Tagging

- Tags are now associated with a user-defined color. Reviewers can use tag colors to visually group tags. For example, one could make all topic-oriented tags green, all processing-related tags blue, and all confidentiality-related tags red. Tag colors are shown in the Tags facet, in the Previewer, and in the new Tag Colors table column. This column gives a visual overview of an item's tags by displaying all associated tag colors.

- The Add Tags and Remove Tags menu options in the Details views have been replaced by a single Edit Tags menu option.

- The Rename Tag menu option in the Tags facet has been renamed to Edit Tag.

Redaction

- Added the ability to overlay a text on a redacted area, e.g. to indicate the reason for redacting that area.

- Added the ability to define redaction templates. Such templates bundle a set of visual redaction settings, such as color, overlay text, and overlay font, and give it a symbolic name, e.g. "privileged content". This lets one centrally manage the visual style for a specific type of redaction. The items redacted with a specific redaction template can be retrieved via the Features facet. Redaction templates can be carried over to other cases using the Case Template functionality.

- Added the ability to use a custom color for mass redactions.

- Added an option to draw a border around white redactions.

- Added an option to render all redactions in black upon export.

Reporting

- Added an optional Table of Contents.

Exporting

- Resolved the exporting of the event log to an XLSX file failing due to cells that reach Excel's maximum cell text length limit.

Exporting – PDF

- Improved exporting of MS Office files to PDF/TIFF.

- Improved exporting of chat messages to PDF/TIFF.

Exporting – Item Reports

- Added Case Name and Case Created custom fields.

- Added the ability to add custom logos.

- Improved the rendering style of hyperlinks in the reports.

- Improvements that make it easier to reuse report templates across cases.

- Resolved an issue with the inconsistent use of bold fonts in the Table of Contents.

- Resolved an issue with certain images failing to export to a report.

Exporting – Load Files

- Added the ability to export time zone offsets and time zone names.

- Resolved an issue with PDFs containing certain types of form fields not exporting to TIFF correctly.

Intella TEAM

- Resolved an issue with redactions failing to store.

- Resolved an issue with queries launched from the Internet Artifacts section in the Insight tab resulting in an error and failing to evaluate.

Dongle Manager

- Resolved an issue with the Blink button no longer working.

Upgrade Notes

Intella 2.3.1 can directly open cases made with Intella 2.3, 2.2.x, and 2.1.x.

When a case made with an older Intella version is opened in Intella 2.3.1, adding Custom ID tasks to the case in version 2.3.1 may render the case unopenable in that older version. Changes have been made to prevent such forward compatibility issues in future releases.

The Raw Data field names for items extracted from a Cellebrite report are now all in lowercase. This may affect rules for deriving custom columns. A new option has been introduced to make the check for a given field name case-insensitive.

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 2.3.1 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.