Intella 2.1 Release Notes

Highlights

- **Email threads** are now detected and visualized. This includes the determination of the **inclusive emails**: together these cover all the content in the thread. This can reduce review time and effort. **Missing emails** are highlighted in the thread.
- **Identities** modeling lets one build an “address book” of the persons of interest, bundling their aliases such as email addresses, phone numbers and chat accounts into a single unit. Various facets and displays use this to improve their content.
- Added an **integrated OCR** option. All Intella users can now OCR documents and images without requiring additional software, licenses, or systems.
- Added **recovery of deleted files** in NTFS disk images using the MFT.
- Added functionality for **removing sources** from a case.
- **Custom columns** let one extend Intella’s data model with new columns, populated by selected headers, raw data fields or load file columns.
- Added support for the **Ext4** file system.
- Added support for indexing non-encrypted **iTunes backups**.
- Improved the **presentation of instant messages** by bundling them in day-to-day conversation items.
- The **Social Graph** now also shows phone calls and instant messages. When any of the aliases are found in an Identity, these nodes are merged. This presents a unified view of the communication between people, regardless of the communication medium used.

General

- The Intella 2.1.x version range will be the last range to support installation on a 32-bit Windows platform. Starting with Intella 2.2.x, a 64-bit platform will be required.
- Several performance and stability improvements in reading and writing case files, for both local and network file systems.
- Improved a potentially misleading error message related to a failed backup.
- The 32-bit edition of Intella now issues a warning when attempting to index or export data. As these tasks are very memory-intensive, use of the 64-bit version is strongly recommended.
- Improved temp folder management when indexing.

Case Management

- Cases that can only be opened in “review only” mode are now labeled as such in the Case Manager.
- It is no longer possible to open the Add New Source wizard in a review-only case.
- One can now “tab” through all fields in the Add New Case window.

Indexing – General

- Sources can now be removed from a case.

- It is now possible to define custom columns. This allows one to extend the data model of an Intella case with new columns, based on values found in the Headers or Raw Data tabs. For example, one can create a custom column to show the “X-Mailer” header value as a “Mail Client” column.
  Custom columns are typed, e.g. as a string, number, or date. This ensures a proper sort order when sorting on that column. The data in custom columns is generally searchable using keyword search. Custom columns that use the date type can be found and queried in the Date facet.
- Added support for indexing non-encrypted iTunes backups. This was tested on iTunes 12 with a variety of iOS versions. Other iTunes versions are being tested.
- Item IDs now stay the same when re-indexing a case.
- Many stability and performance improvements for indexing PDF documents. This results in more and better extracted text and images, faster extraction times and improved resilience to broken data.
- Improved indexing speed on large SQLite files.
- Improved the processing of TNEF attachments (winmail.dat files).
- Added detection of Apple icon (.icns), Radiance High Dynamic Range RGBE Format (.hdr) and DjVu (.djvu, .dvj) images.
- Geolocation references that are embedded in Google Maps URLs are now extracted and can be displayed in the Geolocation views.
- Improved paragraph hashing, resulting in better detection of duplicate paragraphs. A number of search features benefit from this.
- Improved modeling and normalization of the sender and receiver information of instant messages and phone calls.
- Resolved a concurrency issue that could occur when indexing PST files.
- Improved type identification of Bloomberg plain text documents.
- Improved processing of hierarchical generic Notes documents.
- Improved determination of the Source IP address of emails.
- The NSF document UID is now logged before processing that NSF item. This can help diagnose NSF items that fail to index.
- Improved resilience for NSF files containing items on which Notes crashes.
- Resolved an issue with MBOX and EML files originating from MacOS platforms not indexing correctly due to their end of line encodings.
- Resolved an issue with the longitude and latitude properties of items in an XRY phone dump not being extracted.
- Resolved an issue with the sorting on primary or family dates that could produce an incorrect sort order when the primary date preferences were changed and the user canceled the subsequent recalculation of these dates.
- Resolved an issue with incorrectly processed MMS messages in XRY phone reports.

Indexing – Disk Images

- Intella can now extract deleted items from disk images. File recovery is currently restricted to NTFS file systems and is based on traces of the deleted files found in the Master File Table (MFT). Intella tries to recover as much as possible of the file content and metadata. Whether a full or even partial recovery is possible depends on how the disk was used after the file deletion. Note that this functionality does not scan the unallocated space or slack space.

- Added support for the Ext4 file system.
- Added support for MacQuisition disk images (IMG format).
- Cellphone reports and IBM Sametime dumps can now also be indexed when they are contained in a disk image. Previously, they had to be present in the local file system.
- Resolved an issue with indexing file system roots in AD1 disk images.
- Resolved an issue with the indexing of disk images mounted as a virtual drive with EnCase.
- Various stability improvements for indexing disk images containing an NTFS file system.
- Resolved an issue with DD disk images consisting of more than 99 parts that would not index properly.

Indexing – Load files

- When importing a load file, it is now possible to define custom columns. This allows one to extend the data model of an Intella case with new columns. Contrary to the global Custom Columns feature, here the new columns are populated with selected columns from the load file, allowing any type of load file to be imported fully into an Intella case.
  Custom columns are typed, e.g. as a string, number, or date. This ensures a proper sort order when sorting on that column. The data in custom columns is generally searchable using keyword search. Custom columns that use the date type can be found and queried in the Date facet.
- Improved the importing speed of load files containing custodian columns.
- When processing the content of binary items bundled with a load file, one can now specify the same configuration options as when adding a source, e.g. whether item recovery should be used, whether archives should be expanded, etc.
- The unit of the Size column can now be bytes, kilobytes, megabytes or gigabytes.
- Improved importing speed through better utilization of CPU cores.
- The import configuration is now logged when importing a load file.
- Items with empty content (zero byte files) no longer get a message hash.
- Resolved an issue with documents getting typed incorrectly when they had an incorrect file extension and the binaries were available for proper file type detection.
- Resolved an issue with load files containing MSG files getting incorrect message hashes.

Indexing – Cloud Sources

- Improved robustness and error handing of all cloud sources.

Content Analysis

- Improved content analysis speed. Typically, computations can be up to twice as fast depending on the CPU type, except for skin tone analysis.
- Added support for various image types in skin tone analysis.
- The item field(s) on which content analysis is applied can now be specified. Before, content analysis could only be done on the document text.
- Resolved an issue with incorrect match highlighting in the Regular Expression Assistant’s sample text.

- Resolved a UI layout issue in the Regular Expression Assistant when using Windows font scaling at a value larger than 100%.
- Resolved an issue with content analysis calculations proceeding when Intella was shut down.

Email Threading

- Added functionality for threading a set of emails. This process determines the “reply”, “reply all” and “forward” relationships between emails, based on metadata found in the email headers, the email container or embedded in the email body.
- The resulting sequence or tree of emails is displayed in the Email thread tab in the Previewer, with an indicator of where the current email is located within its thread.
- Mails that are referenced in the email metadata but that could not be found in the evidence data are marked as “missing emails”. An example is a mail with an In-Reply-To header that refers to another mail that is not present in the current evidence set.
- The “inclusive” mails are determined and highlighted in the Email Thread tab. These are the mails that *together* contain all content present in the thread. Having read all inclusive mails implies having read the entire thread. This can be used to improve the time needed to review a large collection of emails.
- The determined threads are listed in the new Email Thread facet and can be used as queries.

Identities

- A new top-level tab called “Identities” has been added. The functionality in this tab can be used to organize all aliases used by a specific person or organization in their communication, e.g. the various email addresses, phone numbers and instant messaging IDs used by a person.
- This information is used to improve the display of values in the respective facets and other displays. For example, the Email Address facet will group the addresses by identity, letting the user query for all the identity’s addresses at once. The Social Graph will combine the nodes representing those email addresses and bundle them into a single node, reducing the graph complexity and painting a more accurate picture of the communication flow.
- An Identity facet has been added, allowing for the querying of all communication of an identity, regardless of the communication media and addresses used. This allows for following a conversation that is taking place across multiple channels.
- Intella can show a list of suggested identities, based on patterns found in the evidence data such as similarly looking email addresses. Identity information can also be added manually.

Tasks

- A task condition called “OCR Candidates” has been added. This can be used to gather e.g. all documents and non-embedded images. This way they can be conveniently OCR-ed, tagged or exported. The condition can be configured to focus on specific types of documents and images, whether it should be limited to empty documents (not containing any text), etc.
- Resolved an issue with the match all/match any drop-down list incorrectly initializing its value when editing a task.

OCR

- Added an integrated OCR engine (ABBYY FineReader) to Intella. This lets users OCR items directly from within Intella, without requiring any additional software, systems, or licenses. This functionality is available in all Intella editions, regardless of the license type.
- The OCR text is now shown in a separate tab in the Previewer; it is no longer part of the Contents tab. It is still subject to full-text search, this is only to make it clear where the text originates from.
- When OCR-ing items, one can now indicate what to do with items that already have been OCRed: either skip them, or replace the old OCR text with the new OCR text. Previously, the OCR text would be appended to the currently stored text, which may include the results from a previous OCR job.
- Resolved an issue with OCR results not getting imported properly.
- Improved OCR speed when using ABBYY Recognition Server.
- The OCR task in the Insight tab's Workflow section now uses the same logic as the OCR Candidates task.

Searching

- The "Export" search field has been renamed to "Export ID".
- Added an "Has Attachments" category to the Features facet.
- Added a "Batched" category to the Features facet, containing the items that have been assigned to a coding batch in Intella Connect.
- Registry artifacts can now be skipped when searching for the direct and top-level parents in the item hierarchy. See the Search tab in the Preferences window.
- Resolved an issue with saved searches referring to items that no longer exist after a re-index.
- Resolved an issue with visualized tag queries not updating their result sets after a re-index.
- Resolved an issue with Ctrl-clicking and Shift-clicking not working in certain facets when the facet was being filtered using user-entered text.

Results

- Added a Geolocation column to the Table view, reporting the longitude and latitude of items such as digital camera photos.
- Added a Conversation Index column, reporting the PR_CONVERSATION_INDEX property or Thread-Index header.
- An "Analysis" table column group has been added, containing columns that indicate items whose content has been processed by content analysis, email threading and OCR.
- A divider can now optionally be drawn in the Table view, dividing the rows into groups that have the same value in the sorting column. For example, one can group items on their email subject line. Note that not all columns support this divider.
- The CSV export option can now export arbitrary fields from the Raw Data section of an item. An example use case is exporting of the PR_... MAPI properties of the selected items.

Previewer

- Instant message types such as SMS, MMS, iMessage and the various chat clients supported by the cellphone extraction tools are now processed similar to how Skype messages are processed and displayed: all messages between two people or in a group chat are combined into items that cover the messages of a single day, with the option to navigate to the previous and next day in the conversation. This improves the ease of review of such instant message types.

- Added support for natively previewing OpenDocument documents.
- Removed the preference for the maximum number of pages limit. This used to limit the maximum number of pages shown in the Preview tab. In its place comes a preference for the maximum file size, which defaults to 10 MB.
- Many improvements in rendering PDFs. This also affects the Preview tab for other item types, such as MS Office documents.
- CSV and XLS files now render with auto-fitting of columns in the Preview tab (optional for XLS).
- Added support for previewing and exporting various image file types: Windows icons (ICO files), HDR, Apple icons (ICNS), IFF, PCX, Photoshop (PSD), SVG, WMF/EMF (partial).
- For XLS files, text is no longer truncated using scientific notation in the Preview tab, unless the cell in the original file is set to use scientific notation.
- The Headers tab now preserves the indentation in the header text.
- The PR_MESSAGE_FLAGS value in the Raw Data tab now shows a human-readable value.
- Resolved an issue with the Previewer not showing the Attachments tab when viewing calendar items.
- Resolved an issue with the Words tab listing duplicate words.

Social Graph

- The Social Graph has been extended to support all forms of communications. Before it was limited to showing only emails. Now, it also supports phone calls and chat messages (SMS, MMS, iMessage, Skype, etc.).
- The Social Graph now merges address nodes occurring in the same identity – see the Identities section for more information. This reduces graph complexity and improves the informational value of the display.
- An "Edges" filter has been added with three possible states: "All", "At least one Identity" and "Only Identities". This can be used to filter out edges that do not involve identities. This is useful in cases where sufficient effort went into the modeling of identities and the communication with other addresses is no longer of interest.

Tagging

- The tag hierarchy can now be rearranged, i.e. the parent tag of a tag can be changed.

Keywords tab

- Resolved an issue with keyword queries containing wildcards always reporting "0" in the Hits column.

Redaction

- Changed the settings in the default redaction profile so that only limited metadata is contained in exported redacted items.

Exporting – Original Format

- File names are no longer truncated to 120 characters when exporting on Windows 10, as the limits for file name lengths have been increased on that platform.
- Resolved an export error that would occur when exporting items typed as “Email Headers”.

Exporting – PDF

- The pages can now be numbered automatically.
- Added support for Open Type font (OTF) files.
- Various fixes and improvements for exporting MS Office files to their native rendering.
- Resolved an issue with redacted attachments and embedded items being exported incorrectly.
- Resolved an issue with (partially) transparent pixels in PNG files being rendered incorrectly.

Exporting – PST

- One can now export directly to the PST root folder.
- Resolved an issue with MSG files contained in a ZIP file that could not be exported to a PST file.
- Resolved several issues where specific types of calendar files could corrupt the PST file they were being exported to.

Exporting – Load Files

- All PDF exporting improvements apply to the exporting of load files as well.
- Added an “Has extracted or OCRed text” field.
- When exporting items as images in a non-PDF format (e.g. TIFF or PNG), PDFs can now optionally be generated as well.
- Added support for exporting to Multi-page TIFFs.
- One can now export arbitrary fields from the Raw Data section of an item. An example use case is exporting of the PR_... MAPI properties of the selected items.
- When skipping items, the document type can now optionally be mentioned in the placeholder text.
- The unit of the Size column can now be bytes, kilobytes, megabytes or gigabytes.
- Added the Page Count field to Opticon (OPT) files.
- Resolved an issue with an incorrect load file being created when export errors occurred.
- The “Relativity” load file format is no longer marked as “experimental”.

Upgrade Notes

Intella 2.1 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 evidence is re-indexed 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.

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 takes considerable time, comparable to what it took to index the original case.

Case conversion will also 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.