Intella 1.8 Release Notes

Highlights

- Greatly improved **indexing speed**: typically two to four times faster in total indexing time (more on high-end machines), depending on the evidence data and hardware used.
- Several features for searching and displaying paragraphs:
  - Search for **all items containing a specific paragraph**, regardless of item type and small variances such as line breaks and spacing.
  - **Ignore commonly occurring paragraphs** such as email signatures and legal disclaimers. These paragraphs will be ignored during keyword search.
  - Mark paragraphs as "**seen**", causing them to be displayed in a lighter color whenever they are shown.
  - **Collapse and expand** paragraphs.
- Added a user interface for defining **indexing tasks.** This lets the user define compound processing steps such as applying a keyword list and tagging or exporting the results. The primary use is for these tasks to be run automatically after indexing completes, but they can also be manually started at a later point in time.
- Improved **disk image processing**: better speed and more supported file system formats.
- The new **Sets visualization** shows how search results compare in volume, without showing the overlaps between the results. The Sets visualization is available as a mode in the Cluster Map visualization, letting the user choose between these two modes. This new visualization scales to a much larger amount of result sets than the original Cluster Map visualization.
- Simplified the **list of source types** in the Add New Source wizard.
- The Contents tab now captures the **original layout** of the item text better. E.g. tables, font styles and lists are now shown.
- Added support for **Bloomberg** email dumps.
- Improved support for running Intella on **Windows 8.1**.
- Merged the Viewer and TEAM Reviewer products into a single **Viewer** product.
- Added support for using **Lotus Notes 9** for opening NSF files during indexing.
- Many **load file import and export** improvements.

General

- The Intella Viewer and Intella TEAM Reviewer products have been merged into a single Viewer product. This product features all of the old Viewer and TEAM Reviewer functionality.
- This release fixes an issue with the dongle software that may be encountered when running Intella on Windows 8.1. Certain operations could result in an error dialog with the text "Cannot find HASP SRM Run-Time Environment DLL (E0004)". If and where the error occurred depended on the machine that Intella was running on.

Indexing

- Intella's indexing back-end has been rewritten from scratch to make better use of state-of-the-art hardware, especially improving the utilization of modern multi-core CPUs and large

amounts of RAM, while maintaining its ability to run on low-end hardware for less demanding cases. On regular workstations we often see a two- to fourfold speed increase in indexing an evidence data set. On high-end hardware and with further tuning this can be increased even more. The speed improvement is typically greater on larger data sets.

- The list of source types in the Add New Source wizard has been simplified. There is now a "Folder or File" source that merges the following former source types:
  - The Folder source.
  - All single file-based email container sources: MS Outlook, MS Outlook Express, IBM Lotus Notes and Mbox.
  - The Cellphone XML Report source.
- Added an option to analyze the paragraph structure of item texts. See the paragraph functionality descriptions elsewhere for a description of the new functionality that this provides. The option is turned off by default as it incurs some extra processing time; typically around 10% extra time is needed. A future Intella release will add the ability to run this analysis as a post-processing step.
- When the user defines a new source, the Add New Source wizard will show a new wizard sheet titled "Indexing tasks". On this sheet the user can define post-processing steps that need to take place after the source has been fully indexed. These tasks can also later be edited and launched through the Tasks item in the File menu. Each task consists of a condition and an action. Currently the following conditions can be defined:
  - A keyword search, optionally combined with a date range search on all date fields.
  - Same but with a keyword list.
  - Same but with a MD5 list.
  - An arbitrary Saved Search, which effectively can combine all of Intella's search facets.

  The following actions can be defined:
  - Tag all found items with one or more tags. The tag(s) can optionally be inherited by items in the same family hierarchy and/or by duplicates of the found items.
  - Flag all found items.
  - Add a comment to all found items.
  - Export all found items using an export template.
- When indexing a folder of mail containers, only the folder is now considered to be a source (e.g. listed as such in the Source column). Previously each mail container would be listed as a separate source. From now on that will only be the case when the user explicitly defines a mail, load file, cellphone or disk image source.
- During case creation a folder can be optionally be entered for storing temporary indexing data. When this folder is located on a physically separate drive from the evidence data and case folder, this third drive can reduce the total indexing time. Note that the system requirements for this third folder and drive are equal to that of the case folder in terms of available size and speed.
- Various improvements to file type detection.
- Added a dedicated MIME type and Type column value for empty files.
- Lotus Notes 9 can now be used to index NSF files.
- The default path for Lotus Notes is now C:\Program Files (x86)\IBM\Notes.

- The indexing progress screen now mentions how much MB or GB of evidence data there is to be processed and how much of it has already been processed.
- The indexing progress screen now mentions how many indexing steps there are to be performed (crawling the evidence files is just one of the eleven steps), which step is currently being executed and (when available) what the progress of that step is as a percentage.
- Added support for indexing messages in a Bloomberg XML dump. Supported item types are messages, instant messages and related items such as invites and attachments.
- Improved disk image processing:
  - Faster opening and processing of large disk image files.
  - Added support for MacOS, GPT and ISO images.
- Resolved an issue with certain corrupt PDF files causing indexing to run into an infinite loop. This situation was automatically detected and remedied by Intella, but at the cost of reduced indexing speed as the detection of such a situation is based on a time-out mechanism.
- Resolved an issue with disk image files not being processed when the file name contained an apostrophe.
- Resolved an issue with local domain names being appended to the Sender email address of a mail extracted from an NSF file.
- Made text extraction from HTML documents more robust. Note that this also affects email bodies encoded in HTML.
- Many small improvements to text, metadata and image extraction.

Searching

- When the "Analyze paragraphs" option has been selected during source definition, Intella will show extra UI elements in the left margin of the Previewer's Contents tab. These controls mark the start and end of each paragraph and allow the user to collapse and expand paragraphs. Furthermore a popup menu is shown when the user right-clicks on a paragraph, offering the following options:
  - Mark the paragraph as Seen, or back to Unseen. This grays out all occurrences of this paragraph in all items, facilitating the review of large amounts of long and overlapping documents such as email threads with lots of quoted paragraphs.
  - Mark all paragraphs above or below the current paragraph as Seen or Unseen.
  - Search for all items in which this paragraph occurs.
  - Mark the paragraph for exclusion from keyword search. This can be used to suppress information present in lots of items but with little relevance to the investigation, such as email signatures and legal disclaimers. Consequently, keyword queries containing terms such as "confidential" and "legal" are more likely to return meaningful results.
- Resolved an issue with certain phrase queries not evaluating properly.

Results

- In order to scale to visualizing larger numbers of search result sets, the Cluster Map has been extended to offer two distinct visualization modes, called Clusters and Sets:
  - The Clusters mode shows the original Cluster Map visualization that has been a part of Intella since the start.

- The Sets mode is a new visualization that shows each search result as a square whose size is related to the number of items in that result set. The results are furthermore grouped by their order of magnitude, e.g. < 10 items, < 100 items, < 1000 items, etc.
  - The user can toggle between the Clusters and Sets modes.
  - When the graph shown in Clusters mode is too complex to display in a reasonable amount of time, Intella will automatically and directly switch to Sets mode and disable the Clusters mode until the graph's potential complexity in that mode is feasible to be displayed again. Previously such complex Cluster Map graphs could freeze the user interface for some time.
- Empty result sets are no longer shown in the Cluster Map.
- Improved the result set name of keyword list results.

Previewer

- The extracted text shown in the Contents tab now preserves some of the layout attributes of the item text, such as table structures, basic font attributes and lists. This makes it easier to make sense of the extracted text while retaining a key feature of this tab: revealing all of the extracted text. For example, intentionally obscured text such as white text on a white background may be overlooked in the complete native rendering shown in the Preview tab, but will still be clearly visible in the Contents tab. What layout features are shown depends on the item type.
- Redaction improvements:
  - Added a Delete button.
  - Added Undo & Redo buttons.
  - Adding a redaction or editing one no longer requires clicking the corresponding toolbar button: just select an area to add a redaction rectangle and click on a redaction rectangle to move or resize it.
- Hit highlighting improvements:
  - Improved hit highlighting in the Preview tab for certain corner cases.
  - Hit highlighting ignored whether a keyword query was only focusing on specific item parts only, such as the item text, title or creator. This caused items to show "hits" in parts that were not being searched through.
  - Fixed an issue with hit highlighting disappearing after the user clicked the "Show full text" button in the Contents tab.
- The Properties tab now shows the item ID.
- Resolved an issue with the Tree tab not showing any sub-nodes for certain nodes.

Exporting – General

- When exporting calendar entries to a PST file, the names and extensions of any attachments they contain got lost and showed up as "noname.txt" in Outlook due to an incorrect header being set. This has been fixed.
- When rendering a Word document with an auto-date field to its original layout, the current date would always be inserted. This has been fixed.
- Exporting of documents to PDF format no longer requires MS Word to be installed. For spreadsheets and presentations an MS Office installation is still required.

Exporting – Load Files

- Calendar, contact and task items exported to a load file now have a reasonable file extension like ".ics", rather than ".bin".
- Summation load file export now has an option to export a Summation control list (.LST) file.
- Resolved an issue with XML markup being reported as the body of an email in a Summation load file.
- Resolved an issue with missing parent or child IDs. When an item such as a ZIP file contained folders with files in them and both the files and the parent ZIP file were exported, the parent and child IDs would get lost due to the fact that folder items are never exported to a load file. Such items surrounding the folder items are now re-linked during export.
- The "Use transparent numbering in groups" option has been relabeled to "Continue page numbers from previous folder".
- Changed the default image export settings:
    - The Image DPI setting changes from 72 DPI to 300 DP.
    - The TIFF compression setting changes from LZW to Group 4 Fax Encoding (CCITT T.6).

Upgrade Notes

Intella 1.8 is able to open cases made with Intella 1.7.x and 1.8.

Cases in 1.7.x format do not require any case conversion or re-indexing. However, some functionalities and improvements may not be available for such cases. Cases made with 1.7.x cannot be re-indexed or extended with additional sources.

Cases made with Intella 1.6 or older are not supported. One can however use Intella 1.7.3 to convert these cases to the 1.7 format and then open them in 1.8.

Cases made with Intella 1.8 beta 1 or beta 2 are not supported and should be recreated.