Intella 1.9.1 Release Notes

Highlights

- Added an **Insight** view, giving an extensive yet concise overview of **suspect behavior** gathered from browser histories, Windows registries and other sources. Examples are most often visited sites, connected USB storage devices, connected networks, system and service accounts, social media usage (e.g. Facebook, LinkedIn), webmail usage (e.g. Gmail), cloud storage usage (e.g. DropBox, OneDrive), online productivity sites (e.g. Google Docs, Office 365), etc.
- Added support for FTK's **AD1** disk image format.
- Added indexing of the **Windows registry**.
- Added indexing of **browser histories** of all major browsers.
- Added support for **MS OneNote** files.
- Added **text extraction** from unsupported binary files.
- Improved **Type facet** tree structure.
- Extended **keyword list statistics** with user-defined columns.
- Greatly improved **tagging speed**, often 1-2 orders of magnitude.
- **Indexing speed** improvements.

General

- This version incorporates a new icon set.
- The audit trail functionality has been replaced by an exportable event log. The binary events.log file, which has been around for some time and holds all information of the audit trail, can now be exported to a CSV file. When exporting the events, one can choose what types of actions need to be exported (e.g. related to tagging, indexing or exporting), filter events by date and restrict the exported events to particular users only.
- Certain harmless error messages in the log file, e.g. about search operations being cancelled during application shutdown, are now suppressed.
- Several minor user interface improvements.
- Resolved an issue with a case containing an IMAP source that refused to open.
- Improved the help text accompanying the case backup option.

Indexing

- Added optional indexing of all keys and values in the Windows registry. When turned off, the extraction of particular artifacts necessary for the Insights tab (see below) will still take place.
- Added optional indexing of browser histories. Supported browsers are Internet Explorer/Edge, Chrome, Firefox and Safari.
- Added optional extraction of human-readable text from binary files whose file type is not recognized or supported by Intella. By default this option is turned off due to the impact it has on indexing speed and case size and because the outcome may be noisy and require forensic insight to interpret correctly.

- The Items sheet in the Source wizard has been extended with additional options, giving greater control of the types of items that Intella will index. Previously this sheet would let the user toggle the processing of mail archives, file archives, embedded content in documents and deleted emails. New options are:
    - Chat messages – controls the processing of Skype and Pidgin databases, Bloomberg XML dumps, WhatsApp messages in cellphone reports, etc.
    - Databases – controls the processing of non-Skype SQLite databases.
    - Windows registry – see above.
    - Browser history – see above.
    - The deleted emails option has been extended to cover Notes deletion stubs as well.
    - Text fragments from unsupported and unrecognized file types – see above.
- Added support for MS OneNote Notebooks. Supported versions are OneNote 2010, 2013 and 2016.
- Added support for Mac OS property lists (.plist files). The ASCII, XML and binary variants are all supported.
- Improved detection of MS Office formats, relying less on known file extensions.
- Added support for AD1 (v3 and v4) disk images.
- Added support for ExFat file systems.
- Added support for the LZMA2 and PPMd compression methods.
- Added support for XZ archives.
- Improved support for broken ISO archives.
- Added support for indexing Pidgin chat logs and accounts.
- Various indexing speed improvements, e.g. better multi-threading on disk image indexing, reduced overhead on large sets of loose files, reduced indexing time of very large archives, removed multi-threading bottlenecks on NSF files, cellphone report and Sametime dumps.
- The check on start-up for the availability of the evidence files has been made optional on a per case basis.
- Several refinements to EDB file processing.
- Several refinements for rendering and text extraction of MS PowerPoint files.
- Several refinements to the indexing of SQLite databases.
- Improved processing of generic Notes documents.
- The list of indexing tasks can now be reordered.
- Conditions in a task definition can now optionally deduplicate the determined set of items.
- Verified that files made with MS Office 2016 will index properly.
- For File and Folder sources the Attach Evidence dialogue now allows for the selection of evidence files. Previously it would only support the selection of folders.
- Resolved an issue with indexing tasks defined during source definition not being stored correctly. This affected cases where multiple sources were defined in sequence and indexed all at once using the “Re-index” button.
- Custodian names can now be changed.
- The UI will no longer let the user enter a custodian name containing the slash character (‘/’).
- Resolved an issue with the “Include subfolders” and “Include hidden folders and files” options in a File or Folder source being ignored.
- Resolved an issue with certain HTML and XML files not being classified as such.

- Resolved an issue with HTML files using UTF-16 encoding failing to index.
- Resolved an issue with UTF-16 text files containing non-ASCII characters not being classified properly.
- Resolved an issue with indexing becoming unstable when encountering IBM Notes deletion stubs.
- Resolved an issue with crawling terminating immediately when a single file or folder in the evidence folder is being denied access to.
- Resolved an issue with the associated phone number file not being taken into account when indexing an UFDR cellphone report.
- Resolved an issue with the importing of load files containing images in PDF format.
- Resolved an issue with the importing of load files causing existing tag group columns to disappear.
- Resolved an issue with importing load files that contain hierarchical tags.
- Resolved an issue with certain PDF metadata fields not being full-text indexed.
- Resolved an issue with the port configuration of an IMAP source not being used.
- Resolved an issue with certain encrypted NSFs not being detected as encrypted, causing the decryption step to be skipped.
- Resolved an issue with encrypted (and possibly decrypted) NSF files not being marked as such in the results list and item properties.
- Resolved an issue with the importing of OCR-ed items replacing rather than extending the existing stored text for those items.
- Resolved an issue with Window directory junction file system links being followed during crawling.
- EDB sources are no longer labeled as “experimental”.

Searching

- The tree structure of the Type facet has been reorganized to make it easier to oversee and to better suit investigator needs.
- Added an “All Items” branch to the Features facet.
- The Saved Searches facet now has a separate branch for the default saved searches, keeping them separated from the user-defined saved searches. The “Default searches” node is the first in the list, followed by the user branches in alphabetical order.
- The Keywords table in the Statistics view can now have columns representing saved searches. This allows for the creation of a matrix where a keyword list can be compared against virtually any other aspect (or combination of aspects) that one can query on, e.g. a date range, a tag, item type, review status, etc.
- The accounts in the Chat Account facet now have a suffix indicating the chat client, e.g. Skype, ICQ, Jabber, …
- Resolved an issue with the Delete menu option in the Saved Searches facet becoming inactive.
- Improved handling of unusual quote characters in keyword queries.
- Resolved an issue with Intella crashing when entering non-existing dates in the Date facet.
- Resolved an issue with the Show Parents search option not functioning correctly on items originating from DD disk images.

Results

- Added an Insight tab to the main window, giving a concise and exportable overview of suspect behavior gathered from browser histories, Windows registries and other sources. The Insight tab holds the following information:
    - Basic case information such as creation date, location and evidence size.
    - Various total and deduplicated item counts: all items, encrypted & decrypted, exceptions, recovered items, …
    - A quick overview of encountered item types and their volumes.
    - A visualization of the item volume per custodian.
    - Top 100 visited URLs and Top 100 visited domains, per browser history as well as cumulative for the entire case.
    - A breakdown of visited URLs w.r.t. social media usage (Facebook, Twitter, …), cloud storage (DropBox, OneDrive, …), webmail (Gmail, Hotmail, ..) and productivity (Google Docs, Office 365, …). The statistics can be shown per browser history or cumulative for the entire case.
    - A timeline of dates encountered in the evidence.
    - An overview of detected user accounts (Windows, Skype, …).
    - A summary of the most used email addresses and email server host names.
    - Notable registry artifacts, e.g. network interfaces, recent files, shellbags, …
    - USB Mass Storage Devices that have been connected.
    - Networks that have been connected to; both wired and wireless.
    - A visualization of significant words encountered in the text index.
    - A Workflow section, showing a list of potential next steps to refine the index (e.g. through OCR-ing and decryption) or to start the search and analysis of the case (e.g. by adding keyword lists and saved searches).
- Added a Page Count column. Currently supported are MS Word, OpenOffice documents and PDF. Note that the page count is extracted from the document's metadata, not by counting the actual pages in the document.
- Improved the speed of sorting on Family Date.
- Renamed the "Parent ID" column to "Direct Parent ID" and renamed "Child IDs" to "Direct Child IDs".
- Keyword search results are now updated immediately when the set of excluded paragraphs changes.
- Improvements to the display of items in the List view.
- Resolved an issue with incorrect counts being shown in the Duplicates column.
- Resolved an issue with excluded paragraphs not being taken into account with keyword searches containing wildcards.
- All child items of a cellphone report now inherit the IMEI and IMSI properties.
- Resolved an issue with the Histogram in the Statistics view using overlapping time intervals.
- Resolved an issue with the Language column always showing "Unidentified".

Taggings

- Greatly improved tagging speed, often one or two orders of magnitude.

- The Quick Tag buttons in the Previewer and the tag names shown in the Searches list now take the tag hierarchy into account.
- Improved the display of selected tags in the Tags facet.
- Resolved a regression with the Add Tags dialog not filtering the tags list anymore when entering the name of a tag.
- Exporting of the tags list in the Tags facet now supports hierarchical tags.

Previewer

- The Actions tab now also displays information on tagging, flagging, commenting, redaction and OCR actions that have taken place on the item. The timestamp is no longer displayed. To obtain this information, one can use the new event export functionality.
- The Contents tab now scrolls horizontally if necessary when navigating from keyword hit to keyword hit, in order to fully reveal the hit.
- Typing Ctrl+P now triggers the Print Tab function.
- Several improvements for displaying PDFs.
- Resolved various hit highlighting issues, e.g. with phrase or proximity queries containing nested Boolean expressions, queries involving escaped wildcard characters, text fragments including HTML markup symbols.
- Resolved the display of Skype messages sometimes lacking avatars.
- Several item loading and hit highlighting performance improvements.
- Resolved an issue with the Previewer producing an error when viewing certain chat messages.

Exporting – General

- A “Redacted items” sheet has been added to the Export wizard. The available options in this sheet depend on the chosen export format:
    - For Original Format export:
        - “Use redacted images when available” checkbox.
        - “Suppress redacted items” checkbox.
    - For PDF export:
        - “Use redacted images when available” checkbox.
    - For PST and i2 iBase/ANB exports:
        - “Suppress redacted items” checkbox.
    - For Load File export:
        - “Use redacted images when available” checkbox.
        - “Suppress natives for redacted items” checkbox.
        - “Suppress text for redacted items” checkbox, with a sub-option for specifying a placeholder text.
- Resolved an issue with the Print Report function not including the original document view when invoked on emails.
- Resolved an issue with incorrect file extensions being added to the names of exported files.
- Resolved a regression with the “Export values…” in the Export Sets facet no longer working.

Exporting – CSV

- Added an option to set the maximum length of the text in a cell to 32,000 characters. This appears to be the limit imposed by MS Excel. Cells with more than this amount of characters typically spill over to the next row when viewed in MS Excel, breaking the structure of the CSV.

Exporting – PDF

- Added an option for controlling whether OCR-produced text for images is exported.
- Resolved an issue with pages being scaled incorrectly when the evidence page format and export page format do not match.
- Several improvements for displaying MS Office documents.
- Resolved an issue with the "Original view, x pages (displayed on pages y to z)" line in the produced PDF not being translated when the Intella UI language is set to a language other than English.

Exporting – PST

- Improved exporting of emails containing a broken plain body and a correct RTF body.
- Added support for exporting to PST with MS Office 2016 installed.

Exporting – Load Files

- All changes related to PDF exporting.
- Added the ability to configure what the extracted text should be composed of. One can choose to export Properties, Main properties above body, Contents, Headers and Raw Data, in any possible order.
- Added three new custom field types:
    - EXTRACTED_TEXT
    - BEG_ATTACH
    - END_ATTACH

Intella TEAM

- Improved support for user names containing non-ASCII characters.
- Resolved an issue with logging in with Intella Viewer on a case shared by Intella Connect where the server has been configured to use LDAP.
- Resolved an issue with the Edit Tag option being disabled mistakenly.
- Resolved an issue with Intella TEAM Manager 1.9 failing to share a case made with Intella 1.7.x.
- Resolved an issue with the Export Work Report function failing to produce a work report.

Upgrade Notes

Undo Actions and action timestamps – To realize the much-desired tagging speed improvements, it was necessary to disable the Undo Actions functionality and the timestamps column in the Previewer's Actions tab. This functionality may be reinstated in a future release. As a workaround, exporting of the event log to CSV format may provide most of this information.

Backwards compatibility – Intella 1.9.1 can open cases made with the Intella 1.7.x, 1.8.x and previous 1.9.x versions. Cases made with beta versions are not supported and should be recreated.

Cases made with Intella 1.7.x or Intella 1.8.x do not require any case conversion or re-indexing. However, some functionalities and improvements may not be available for such cases.

Cases made with Intella 1.7.x cannot be re-indexed or extended with additional sources. These restrictions do not hold for cases made with Intella 1.8.x, i.e. they can be re-indexed and have new sources added to them.

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 Intella 1.9.1.

While we aim to ensure full backwards compatibility with older cases and older Intella versions where we reasonably can, opening a case made with an older Intella version in a newer version may result in that case no longer opening properly in the older version. We strongly recommend to always create a backup of the case before upgrading.