

Intella 2.0 Release Notes

Highlights

- Updated and **modernized the user interface**.
- Added a **Geolocation** results view, showing the geographic locations of search results, e.g. based on GPS data and IP addresses.
- Added a **Histogram** results view, showing the date distribution of search results.
- Added a **Review** tab, for convenient viewing of all items in a set.
- Added new cloud sources: **Dropbox, Office 365 (incl. OneDrive), SharePoint, Gmail**.
- Added indexing of **virtual machine** images (VMDK and VHD formats).
- Completely redesigned user interface for **importing load files**.
- Added detection of **Bitcoin** cryptocurrency files.
- **Indexing performance** improvements, both raw indexing time and when adding additional data to a case.
- Added **regular expression**-based detection of text patterns, e.g. bank account numbers. A **Regular Expression Assistant** is included for constructing the expressions, together with a library of example expressions.
- Added **skin tone analysis** of images.
- Added several **table columns**, e.g. covering the number of recipients of emails and other communications, passwords and certificates of decrypted items, and others.
- Added a **Recipient Count** facet.
- Refined the classification of **embedded items**, and consequently improved the suppression of **irrelevant items** using this improved classification.

General

- Intella 2.0 offers an updated and modern user interface.

Case Management

- Improved the handling of corrupt cases, increasing the chance of being able to open them. While corrupt cases can no longer be relied upon for future use, this might let the user salvage any work product from the corrupt case.

Indexing - General

- The minimum and recommended amounts of memory required for indexing have been increased.
- Added support for virtual machine images in VMDK (VMware) and VHD (Hyper-V, VirtualBox, XenSource, ...) format. See the User Manual for restrictions on file formats.
- Added detection of Bitcoin wallets and blockchain files. Supported Bitcoin applications are: Bitcoin, Dogecoin, Litecoin, Multibit Classic and Multibit HD.
- Added support for ZIPX files.
- Added support for ISO images in UDF format.
- Indexing performance improvements:

- Improved parallelization inside and between crawler processes and smarter file usage improves the overall indexing time for new and re-indexing cases. Speed improvements up to twice as fast have been reported.
- Other improvements specifically targeted the time needed for the “Index new data” operation. Adding a few files to a large case is now a lot faster. Speed improvements up to four times as fast have been reported.
- The cost of the “Analyze paragraphs” indexing option has been greatly reduced. The option now typically imposes a cost of < 10% of the total indexing time.
- The “Index content embedded in documents” option has been replaced by the “Index images embedded in emails and documents” option. Differences:
 - The new option affects the processing of child items found in documents (Word, PDF, etc.) and emails. Previously it would only apply to documents.
 - The notion of “embedded” and “attachment” has changed. Previously, all direct child items of documents would always be classified as “embedded item”, and all direct child items of emails would become “attachments”. Now it depends on whether the item is an image and how that image is handled when its parent item is displayed. When the image is visible as part of its parent’s native rendering (commonly referred to as an “inlined image”), it is now classified as “Embedded image”. All other child items, including any non-inlined images, are classified as “Attachment”.
 - Where necessary, Intella will stay on the safe side. For item types where the native application typically supports the inline display of images but Intella does not, all child items are classified as “Attachment”. Examples are images that are part of a Contact in a PST file. This matters as the “Embedded image” category is now also part of the suppressed set of items when the “Hide Irrelevant” option is turned on, see below.
 - As the new option now also applies to inlined images found in emails, the performance gain obtained by turning this indexing option off will typically be larger than before.
- Added an option in the preferences to check for the presence of the case’s evidence files on opening of the case.
- Added support for indexing virtual files in disk images, such as the Master Boot Record.
- Several improvements to the processing of MS Office files.
- Several improvements to the processing of RTF files.
- Several improvements to the processing of cellphone dumps.
- Improved the body selection algorithm for emails in PST, MSG and EDB files that have their body stored in multiple formats (plain text, HTML and/or RTF).
- Missing items in a PST file are now recorded in the Exception Items category in the Features facet.
- Extended the metadata extracted from JPEG images and improved the processing of JPEG metadata containing non-ASCII characters.
- Added extraction of metadata from PNG, GIF, BMP, TIFF, WebP, PSD, ICO and PCX image files.

- Improved the accuracy of IBM Notes NSF file type identification, reducing the number of false positives.
- Added support for detecting Adobe FrameMaker files.
- Added support for detecting PCF and ICO image files.
- Added support for Lotus Notes ID files with non-ASCII identity names.
- The Suggest button in the Case Editor now uses the last used parent folder as a location for the new case folder.
- The user interface for importing OCR-ed items now shows the number of failed items at the end of importing.
- Improved error reporting when indexing a folder source and part of the folder cannot be read due to lack of access rights.
- Improved the default name given to disk image sources.
- Resolved an issue with indexing email metadata in PST and MSG files, where the contents of the Sender header would be reported as the value of the From header.
- Resolved an issue with indexing getting stuck on processing certain MS OneNote files.
- Resolved an issue with certain types of virtual folders in AD1 disk images not being recognized as such, which had consequences for indexing performance.
- Resolved an issue with disk image indexing failures not resulting in the disk image being registered as an exception item.
- Resolved an issue with PowerPoint documents failing to index properly due to missing embedded images.
- Resolved an issue with the indexing of broken SQLite files resulting in certain temporary files not getting deleted.
- Resolved an issue with images in PDF documents failing to extract.
- Resolved an issue with certain types of dates in PDFs failing to have their time zone parsed correctly.
- Resolved an issue with the Source wizard listing SQLite 2 files being supported. Only SQLite 3 is supported. Also, SQLite 2 files are now properly reported as Extraction Unsupported in the Features facet.
- Resolved an issue with the crawl progress not showing properly when Intella did not have the required access permissions for one or more evidence files.
- Resolved an issue with a case failing to index when indexing via the command line.
- Resolved an issue with very large “paragraphs” blocking indexing when “Analyze paragraphs” was turned on. This could occur when indexing certain types of log files.
- Resolved an issue with Intella moving evidence files out of the evidence folder into the case folder during indexing of a load file or Lotus Sametime chat dump.
- Resolved the “There is an incompatible JNA native library installed on this system” error message.
- Resolved an issue with timestamps in “Zulu time” notation not parsing correctly.
- Due to differences in how the Optimization folder is now used, its recommended free space is now 1 x the evidence size rather than 2 x the evidence size.

Indexing - Cloud

- Added support for indexing Dropbox accounts. Both personal Dropbox accounts and Dropbox for Business accounts can be indexed. File versions can be extracted and are presented chronologically.
- Added support for indexing Office 365 accounts. Retrieved information includes users, user groups, emails, attachments, folders, instant messages and files stored in the associated OneDrive. Intella can also connect to the cloud SharePoint instance associated with the Office 365 account.
- Added support for indexing SharePoint instances. Retrieved information includes basic site and owner information, users, hierarchically nested sites, conversations, posts, attachments, document libraries, and files and folders from the document libraries. Both standalone and on-premise instances can be indexed, as well as instances hosted in the cloud as Office 365 SharePoint services. The following authentication protocols are supported: OAuth2 (for cloud instances), Kerberos, NTLM and basic authentication.
- Added support for indexing Gmail mail accounts. The retrieved information can optionally be restricted to a specific date range. Benefits of using the Gmail connector over the generic IMAP connector are: better performance, more accurate data representation (e.g. folders vs. Gmail's Labels, threads), and a read-only data connection ensuring that no data is altered.
- All cloud connectors support multi-threaded access to the cloud source to make use of the provided bandwidth as best as possible. All cloud connectors feature automatic retry logic, in case retrievals fail due to intermittent network problems or when exceeding the service's throttling policy limits.
- To improve usability, the list of source types in the Source wizard has been divided into two columns: file-based sources and server-based sources.

Indexing - Load Files

- This release offers a completely redesigned user interface for importing load files and load file overlays. The number of load file-specific wizard sheets dropped from 13 to just 3 sheets. The new user interface offers more control options on how the load file is imported, shows a live preview of how the data is parsed, and gives better validation and error messages.
- Intella now bundles Relativity export and import templates that are designed to be compatible with each other, so one can export items out of one Intella case and into another case using these templates.
- When a load file does not contain information to populate the Type column, it can now optionally be derived by Intella from the bundled binary items.
- When adding a load file overlay, the method for matching load file items with existing items in the case can now also be based on the Document ID.
- The node in the Location facet representing the load file is now showing the source name, rather than both the file and source name.
- The "Import ID" column has been renamed to "Document ID". Furthermore, a "Parent Document ID" has been added.
- Resolved an issue with load file import incorrectly deduplicating images and/or texts when the associated items in the load file are also duplicates.

Content Analysis

- Added regular expression-based detection of text patterns, such as bank account numbers, monetary values, shipment tracking numbers, patent numbers, etc. This functionality comes with a Regular Expression Assistant for constructing and testing regular expressions on sample text. This Assistant also offers a library of example regular expressions.
- Added skin tone analysis. This analyzes selected image files for the presence of human skin colors. The images are categorized in Strong, Medium and Weak categories. Supported file formats include JPEG, PNG, GIF and TIFF. Note that the methods used for skin tone analysis are highly heuristic and will typically produce false positives and false negatives.
- The new Money category finds potential monetary amounts mentioned in document texts.
- The new Time category finds potential time-based references like hours, weekdays, dates, references like “after 7 p.m.”, etc.
- All items on which Content Analysis is run are now registered in the “Content Analyzed” category in the Features facet. Previously, only items that had at least one extracted entity were put in this category.
- Resolved an issue with the default content analysis categories (Credit Cards, SSNs, Phone Numbers) not being applied on texts obtained through OCR.

Indexing Tasks

- The user interface for creating tasks has been redesigned, making it easier to define tasks while at the same time allowing for more powerful tasks.
Each task now consists of three parts:
 - One or more search operations, e.g. a keyword search, date search or tag search. Multiple searches can be combined using an AND or OR.
 - Zero or more “item set refinement” operations, applied on the result of the search operation. These operations take an item set as input and produce another item set. Examples are filtering of duplicates, filtering of irrelevant items, finding the parent items. Multiple filter operations can be pipelined here.
 - One or more actions, e.g. tag or export the produced item set.
- Added “Content Analysis” as a task action type. This runs one or more of the Content Analysis processors on the resulting items.

Insight

- The loading time of the Insight tab has improved considerably.
- Optimized the layout of the boxes in the Insight tab.
- The entries in the “Top 100 visited URLs” and “Top 100 visited domains” tables can now be queried for by double-clicking on them.
- Improved the presentation of Insight components that have no data to show.
- Resolved an issue with Internet Explorer cache entities such as cookies being reported as browser history entries.
- Resolved an issue with tasks in the Workflow section not being marked as completed when they were done via a different route, e.g. via the menu bar.
- Resolved an issue with the Insight tab failing to export after a source had been added or the case had been re-indexed in that same session.

- Resolved an issue with certain Insight components failing to refresh automatically when case data changed. They would only update properly when reopening the case.
- Resolved an issue with double-clicking on tree nodes in the Notable Registry Artifacts section resulting in case-wide queries for all User Accounts/Time Zones/etc., rather than the ones specific to the machine represented by that tree branch.
- Resolved minor usability issues.

Searching

- The Statistics view has been removed, its parts being placed elsewhere in the user interface.
- The Keywords functionality, part of the former Statistics view, has become a top-level tab in the main window. This gives it a lot more screen space to work with.
- The Keywords statistics functionality now allows for an arbitrary combination of item text fields (e.g. body, title, location, etc.) to be searched, rather than restricting the search to either a single field or all fields. This brings it in line with how manual keyword search works.
- Added a Recipient Count facet, letting the user query for the number of recipients of communications. The primary use case for this is filtering out all emails, chat messages etc. that are between two parties and no one else.
- When the “Hide Irrelevant” filter is switched on, it now also filters out embedded images. See the Indexing section for how this category is established. This may result in more items being filtered out, which reduces review time when items are typically reviewed in their native rendering.
- Added and changed categories in the Features facet:
 - Has Geolocation – indicates whether a geolocation has been associated with the item, either as part of the original metadata or through an IP geolocation lookup.
 - Text Fragments Extracted – indicates whether heuristic string extraction has been applied on a (typically unrecognized or unsupported) binary item.
 - “Embedded” has become “Embedded images”. The definition of this category and the “Attached” category has been refined. See the Indexing section for details.
 - “Empty document” has become “Empty documents”.
 - “Unsupported” has become “Extraction Unsupported”.
- The nodes in the Location facet tree that correspond with sources can now be sorted alphabetically or by date added. See the “Display and Locale” tab in the Preferences.
- Improved usability of the date picker in the Date facet.
- Resolves various issues with phrase search corner cases.

Results

- A Geolocation results view has been added, showing the geolocation of items on a zoomable world map. Items are grouped in clusters that break down into smaller clusters when zooming in. Map tile data for the first zoom levels has been bundled with Intella. For deeper zoom levels a connection with a tile server is required. Each cluster of items can be clicked, which lists the items in the Details view beneath the map. Geolocations are obtained from:
 - Geographic coordinates stored in the EXIF data of digital camera photos.
 - Geographic coordinates stored in items extracted from cellphones.
 - Email sender locations, using a geolocation lookup of the sender’s IP address.

- A Histogram results view has been added, showing the timestamps of items as a time-based bar chart. The date field(s) on which the chart is based can be selected by the user. By default, the Family Date is used, ensuring that practically every result item will be accounted for in this chart. The Histogram can toggle between showing years or months. One or more bars can be selected by clicking on the bars or dragging in the chart. This will list the respective items in the Details view beneath the chart.
- Added columns showing the number of recipients of communications such as emails, chat messages and phone calls:
 - Recipient Count – counts all recipients.
 - Visible Recipient Count – excludes email Bcc recipients.
 - Bcc Count.
- Added Password and Certificate columns, showing the credentials that have been used to decrypt an encrypted item. The values shown here are subject to full-text search, as part of the Summary field.
- Added a Source IP column.
- Added a Has Geolocation column.
- Added a File Extension column.
- The “Embedded Item” column has become “Embedded Image”.
- Resolved an inconsistency in the Page Count column. It now makes a proper distinction between “zero items” (showed as “0”) and an unknown page count (shown as an empty cell).
- Resolved an issue with a checkbox for cell text truncation showing in the table column chooser. This functionality only affects the CSV export of the table and should only have been visible in the corresponding export dialog.

Previewing

- Added a Review tab, combining the Details list and an embedded Previewer into a single window. The result is a user interface that allows for convenient browsing of a list of search results without double-clicking and having to handle a lot of Previewer windows. The Review tab can be launched by right-clicking on elements in the Results or Details view and selecting “Review n items”. This opens a new top-level tab in which the selected items can be explored. One can have multiple Review tabs open simultaneously.
- Added a Geolocation tab, which shows the geolocation associated with the item on a geographical map.
- The Properties tab now shows the longitude and latitude coordinates found in EXIF metadata.
- Improved rendering of hierarchical tags through the “Expand top-level tag groups in item properties” setting. When enabled, a Tag hierarchy like “Location” > “USA” will show as “Location: USA” in the Tags line of the Contents tab, rather than “Location/USA”.
- Added support for rendering EMLX files in their native layout.
- Improved navigation of keyword search hits, scrolling the text in such a way that the context of the hit is properly revealed.
- Improved the hit highlighting algorithm for phrase searches.
- Added text wrapping to the Properties tab, making it better able to display long values.

- The “page fit” mode (Fit Width, Fit In Window or Actual Size) of the Preview tab has been made persistent: subsequent displayed items are now shown using the last used mode.
- Resolved an issue with decrypted documents not showing their native rendering.
- Resolved an issue with Intella crashing when right-clicking in the Contents tab.
- Resolved an issue with missing hit highlighting in the Save History in the Properties tab.
- Resolved an issue with the text in OpenOffice documents being rendered in tiny fonts in the Preview tab.

Tagging

- Several usability improvements in the dialogs used for adding, removing and renaming tags.

Redaction

- Added the ability to clear all redactions of an item.
- Removed duplicate information in the default redaction profile.

Event Log

- The Annotation History functionality that was disabled in Intella 1.9.1 due to case database changes has been enabled again in this release.
- When exporting (parts of) the event log, the user is now given the option to export related item IDs to separate text files (one file per event), include the item IDs in the exported file, or skip them altogether. The primary use case of this is to export the IDs of tagged items.
- Added support for exporting the event log to Excel (.xlsx) format.
- Resolved an issue with the event log becoming corrupt when indexing was interrupted.

Exporting – General

- Resolved an issue with the manually entered export destination folder being reset when an export template was selected.
- Resolved an issue with certain social graphs failing to export.

Exporting – PDF

- Resolved an issue with decrypted documents not exporting to PDF in their native rendering.
- Resolved an issue with EML emails attached to other emails that would not render properly in PDF.
- Resolved an issue with the text in OpenOffice documents being rendered in tiny fonts when exporting in original view mode.
- Resolved an issue with certain PDFs having an incorrect document orientation.
- Resolved an issue with export errors related to the creation of the item’s original view not being reported.

Exporting – PST

- Improved support for MS Outlook 2016.
- Several stability improvements.

Exporting – Load Files

- Added an attachment count field.

- When using custom fields, the selected field type and column are now shown in the field chooser table.
- Resolved an issue with the body of redacted emails not being suppressed in Summation load files.
- Resolved an issue with unselecting the “Exclude content” checkbox having no effect.

TEAM

- Added support for opening a remote case on the command line.
- Resolved an issue with a Work Report not being properly restricted to the selected set of items, when requested to do so. Instead, all items would be covered in the work report.
- Several stability improvements, resulting in a higher likelihood of work reports exporting successfully when the case contains broken case data files.
- Resolved an export error caused by illegal MIME type values in the evidence data.
- Improved logging when the TEAM Manager or Connect server can no longer be reached.

Miscellaneous

- Changes to the logging configuration are now effective immediately; it is no longer required to reopen or reshare the case.
- Resolved an issue with harmless yet annoying error messages popping up because of an issue with the Chinese translation files.
- Improved the explanatory text of the error dialog that is used for reporting errors that are not explicitly handled in the code.

Upgrade Notes

Tasks – The storage format of indexing tasks (e.g. for the automated running of keyword lists, applying tags, etc.) has changed. Tasks in existing cases need to be recreated from scratch.

Backwards compatibility – Intella 2.0 can open cases made with the Intella 1.8.x and 1.9.x versions. Cases made with beta versions are not supported and should be recreated.

Cases made with Intella 1.8.x and 1.9.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 or older are not supported.

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.