Intella 1.6.3 Release Notes

Highlights

- Indexing of **disk images** (EnCase E01 and L01 formats, DD format).
- Indexing of Microsoft (**Hotmail**) and **Yahoo** search warrant results.
- Indexing of **nested mail containers** (e.g. a zipped PST attached to an email in an Mbox file).
- Keyword search improvements: search specific **fields** (From, To, etc.), use **wildcards** within phrase and proximity queries.
- Officially supported **64-bit version**.
- Support for **64-bit MS Office and Outlook**.
- Improved **indexing performance**.
- Improved **indexing reporting**: speed graphs, overview of encountered item types and errors.
- Lots of **cellphone**-related improvements, such as XRY's latest XML format.
- Functionalities for **restoring tags** and other annotations from a broken case.
- Added a **Spanish translation**.

General

- The 64-bit version is now officially supported.
- Intella's user interface is now also available in Spanish.
- Several changes improving indexing and search performance, memory usage and stability.
- Fixed the main window's components refusing to resize when dragging the vertical divider.
- Improved the way the software deals with invalid backup paths.
- The backup dialog can now be cancelled, cancelling exiting the application as well.
- Resolved issues with Intella not exiting properly, resulting in files that were kept locked.

Case Management

- The Case Manager now shows currently opened or shared cases as locked and disabled. This prohibits accidentally opening a case that is already open in another Intella process.
- When adding a new case, the chosen case folder path is tested for being a hard disk formatted with the NTFS file system. A warning is displayed when a different type of file system or medium (removable disk, network drive, optical drive) is detected.
- The File menu has been extended with a Restore Annotations menu item. This option can restore the annotations (tags, flags and comments) from a case that has become corrupt (e.g. due to hardware failures or incorrect use of removable drives) into a backup of that case.
- Fixed an issue with the preferences file that could result in the case refusing to open.

Indexing

- Intella can now index EnCase E01 and L01 disk images, as well as images in the DD format. Various file systems are supported, including FAT16, FAT32 and NTFS.

- Added support for XRY's new Extended XML format. This format has been introduced in XRY 6.4 and is strongly recommended over the old format.
- Intella can now index the Hotmail account dumps that Microsoft delivers in response to search warrants.
- Improvements have been made to Mbox indexing to ensure that Yahoo's dumps made in response to search warrants index correctly.
- To speed up indexing, an option is added to the Add Source wizard for turning off storage of the evidence files in the case folder. The drawback of not storing them is that these files need to be available in their original location in order to be exportable.
  Note that items *extracted* from these evidence files, such as emails extracted from a PST file, will always be stored in the case folder. This option is only about the evidence files themselves.
- The indexing progress screen has been extended with a speed graph and more detailed information about the encountered item types and errors. At the end of indexing the speed graph is also stored as a PNG in the logs folder.
- NSF indexing now also detects and indexes orphaned items.
- Mail containers that are not directly located in the file system are now also indexed. Examples are PST files that are zipped or attached to emails.
- The indexing exception report (Sources menu → Exception Report) has been extended and now shows information on problematic sources, as well as various statistics on the types of errors encountered. The report is now in XLSX format instead of the CSV format, to allow for a more user-friendly report that supports all Unicode character.
- When indexing cellphone dumps, the phone number associated with the phone (which is typically not part of the dump) can now be specified using a separate file. This way all calls and messages can have both an Incoming and an Outgoing number associated with them.
- Resolved issues with the file type detection of Cellebrite XML dumps.
- Resolved duplicate indexing of items that are part of an Oxygen XML dump.
- Resolved an issue with Cellebrite SMS messages listing the Incoming number as the Outgoing number.
- Resolved an issue with the Company field and custom properties of MS Office documents not being extracted.
- Resolved an issue with an email body failing to be indexed due to a broken MIME structure.
- Resolved an issue with some facets reporting all categories as empty after a reindex.
- Made the processing of email senders and receivers from PST files more robust w.r.t. syntax and encoding issues.
- Added support for indexing PR_... with multiple values fields in a PST file.
- Resolved an issue with certain NSF emails having incorrect Received dates.
- Message hashes are now also calculated for SMS messages, but only when the sender, recipient and content are all known.
- Resolved an issue with broken XML files triggering an infinite loop, stalling indexing.

Searching

- Wildcards can now be used within phrase and proximity queries.
- One can now explicitly search on specific sender and recipient fields. In older versions these fields were always bundled together in the "Authors & E-mail Addresses" field, making it impossible to search for e.g. a name or address occurring specifically in the From field. With this improvement, the From, Sender, To, Cc and Bcc fields can be searched separately.
- Improved performance of the deduplication operation. This used to be slow on large cases the first time it was invoked.
- Improvements to the keyword search options UI.
- The Type facet's tree now has a branch for disk image types.
- The Show Conversation option now also works on SMS messages.
- Improved the accuracy of the Empty Documents category: some unusual Unicode whitespace characters were not yet supported, resulting in false negatives.
- The Has Duplicates category in the Features facet and the corresponding table column now also take emails into account that have different MD5 hashes but identical message hashes. Before, these would not be returned, even though the Show Duplicates search would return them.
- Resolved an issue with the "Search across all fields" action in the Words tab not always searching across all fields.

Results

- The Details table has been extended with IMEI and IMSI columns, relevant to cellphone data. Furthermore a Device Identifier facet has been added that shows the encountered IMEI and IMSI values and lets the user search for all related items.

Previewer

- Added a scrolling tooltip in the property panel (above the tabs) so that values such as long lists of senders and receivers can be viewed completely.
- The Raw Data tab now also supports the low-level data extracted from NSF emails, MS Office documents and cellphone items.
- Various improvements to hit highlighting in the tabs and property panel.
- All date fields now show an explicit time zone.

Exporting

- The PDF export, the Print command and the Preview tab, which all rely on MS Office for certain file conversions, can now use both the 32-bit and 64-bit versions of MS Office. The bit variants of Intella and MS Office do not have to match. For example, you can use the 32-bit Intella version together with 64-bit MS Office.
- The 64-bit version of Intella can now also export to PST using both the 32-bit and 64-bit versions of MS Outlook. The 32-bit version of Intella still requires that you use 32-bit MS Outlook.
- Removed the Vound branding from the PDFs and TIFFs produced as part of a load file.
- Fixed the order of the columns when the Details table is exported to a CSV file.

- Resolved a MAPI_E_COLLISION error produced by Outlook when exporting to a PST file.

TEAM

- The Work Report functionality has been extended to work across different cases. This lets a user create a case using evidence files already used in another case, and bring over the tags, flags and comments from that other case into the new case. Matching items in the two cases is not trivial as item IDs and paths may be different. Any annotated items that could not be found or not with 100% certainty will be reported.
- The rules regarding who can delete the tags in a case have been relaxed.
  When connected to a shared case, only the creator of a tag used to be able to delete that tag.
  Now, users with a TEAM Manager license can also delete all tags.
  When working with a local case, one can always delete the tags, regardless of who made them.
- Improvements to the tagging progress messages when connected to a shared case.
- A warning dialog is now shown when you attempt to close the case sharing dialog while the case is still being shared.

Installer

- The installer would always remove the last installed set of shortcuts, regardless of the chosen start menu folder. This is problematic when installing several Intella versions side-by-side and removing one of them. This has been fixed.

Upgrade Notes

Intella 1.6.3 can open cases made with all previous Intella 1.6.x versions.

For cases made with Intella 1.6.1 and 1.6.2 there is in principle no need for reindexing the case. Reindexing is only recommended when the original issue had issue that relate to the indexing of the case.

For cases made with Intella 1.6 we do recommend that you reindex if you have not already done so with a more recent Intella version, because of memory usage improvements that require one of the databases to be rebuild.

Please back up your cases before reindexing them.

The first time a case made with Intella 1.6-1.6.2 is opened in Intella 1.6.3, a one-time only database creation process is started. This new database will speed up the deduplication operation considerably. Creation of this database may take several minutes on large cases and slow disks.

Cases made with 1.5.x versions are shown in the Case Manager as needing conversion before they can be opened. The automated case conversion process creates a copy of the case that is subsequently indexed from scratch. The old case is left unchanged and can still be opened with the 1.5.x versions.

Cases made with older Intella versions are not supported.