Intella 2.2 Release Notes

Highlights

- Added support for basic **case merging**.
- Items can now be **exported to a new case**.
- **Case templates** enable quick initialization of a new case.
- Added a **GDPR** Insight info panel, listing privacy-sensitive data found in the case.
- Added command-line options and samples for **scripting** and analysis purposes. Sample scripts are provided that enhance case data using **Google Cloud AI** services.
- Added support for indexing **Windows 10 Mail**.
- Added a **Show Family** search option.

General

- Several improvements to reduce the chance of information loss when processes terminate unexpectedly, e.g. due to a power outage.
- Resolved an issue with cases failing to open due to incorrectly formatted memory settings in the Intella.l4j.ini file.
- Resolved an issue with the Geolocation database presence check resulting in Intella not shutting down properly.
- The executables (Intella.exe and DongleManager.exe) now work properly when invoked on the command line from a different folder than where they are installed.

Case Management

- One can now export items to a case. This can either be an existing case or a new case. Several configuration options are available for controlling what item information is included, e.g. tags, comments, custodians, OCR text, etc. Parents of exported items that are not in the export set themselves are represented as stubs in the destination case.
  The new export functionality supports several use cases:
  - Merging of two or more cases, so that indexing can be spread across multiple machines.
  - Adding data to an ongoing case. The new evidence is indexed in a separate case first, rather than by adding a source to the current case.
  - Exporting of selected items to a new case, e.g. to filter out privileged information or irrelevant items, or to divide the work among reviewers in such a way that each reviewer only has access to their own assigned items.
- The settings of a case can now be stored in a case template. Such a template can be used to initialize the settings of a new case, e.g. to comply with organization policies or to optimize it for the nature of the investigation. Case templates can for example cover:
  - Settings in the Preferences window.
  - Default table column setup.

- Saved Searches.
  - Task definitions.
  - Tags.
  - Keyword and MD5 hash lists.
  - Export templates.
  - Redaction profiles.
- Improved the functionality for adding cases when selecting a case whose case ID or case folder is already present in the cases list.

Auditing

- The Actions tab is now showing the date and time of the events again. This was removed in an earlier version for technical reasons.

Indexing - General

- Added support for the local storage of Windows 10 Mail accounts. Only POP accounts are supported, not IMAP, because only POP accounts store emails locally.
- Updated Skype support to cover versions 7.x, 8.x, 11.x and 12.x. Support for versions 8.x, 11.x and 12.x is still experimental.
- Added support for extracting Chrome bookmarks, cookies, site logins, form history and keyword search history.
- Added support for extracting Mozilla Firefox bookmarks, cookies, and form history.
- Added support for extracting the volume serial numbers and (dis)connect timestamps of USB devices.
- One can now define multiple sources with the same folder path. This supports for example adding the same EDB file twice but with different mailboxes. Another use case is swapping evidence drives between the indexing of two sources that use that same drive path.
- Added detection of Windows Event Log files (EVT and EVTX files).
- Added detection of JSON files.
- Added support for extracting attachments from Notes NSF DXL content. Previously, only inline pictures were extracted.
- Added support for detecting individually encrypted emails in a Notes NSF file.
- Improved the tokenization of texts that contain IP addresses.
- The Source Edit page of an iCloud source can now show the trust token. This is only used when two-factor authentication is used by the account.
- Resolved case indexing errors due to the use of non-ASCII characters in the case folder name.
- Added detection and decryption of loose PGP encrypted files.
- Added detecting and decryption of inline PGP email. PGP mime mail was already supported.
- Improvements for processing Cellebrite UFDR files. Besides fixes for covering e.g. new item types, date formats, etc., a provision has been made so that unrecognized item types are still reflected in the case rather than skipped.
- Several fixes and improvements related to the indexing of MS Exchange EDB files.
- Improvements to the indexing of iTunes archives.
- Improved error reporting and logging when indexing iCloud accounts.

- Improved handling of emails with an invalid character encoding specified in the MIME headers.
- Improved handling of CJK text files (Chinese, Japanese, Korean).
- Improved the Raw Data tab contents of iCloud items, to make it easier to review and to allow for using it as input for custom columns.
- Several improvements in the processing of shell bags.
- Resolved an issue with email body fragments from Mbox files ending up in the logs.

Indexing – Load Files

- Improved importing speed of load files and overlays.
- Load file import no longer adds duplicates in the case when it sees that an item is a child of multiple other items. This change was made because duplicate filtering is typically already done by the application that produced the load file, so these should not be brought back into the data set.
- Cells with formatted numbers (like 1,345,345) can now be parsed.
- Resolved an issue with Intella 2.1.x always enforcing paragraph analysis on imported load files, regardless of the setting chosen by the user.
- Made the import process more robust against character encoding errors.
- Improved handling of empty cells in a load file.
- Improved the validation of load files that use a different encoding than their accompanying text files.

Analysis

- Added a GDPR info panel in the Insight tab. This panel lists categories of information in the evidence data that are of interest from a GDPR compliancy point of view. Examples are person names, phone numbers, email addresses, etc. For each category, the number of values is listed, as well as the number of items holding one or more of these values, further split into Documents/Emails/Other categories. The values can be exported to a CSV or XLS file.
- Added command-line options than enable advanced forms of textual analysis:
    - Added an option for exporting item texts and for importing alternative texts. Imported texts are shown in the “Imported Text” tab in the Previewer, can be found via the Has Imported Text category in the Features facet, are subject to keyword search, and can be exported.
    - Added an option for importing item tags via a CSV file.
    - Added options for finding items based on a keyword search or saved search, and for deduplicating the found results.
    - Sample Windows batch scripts and tutorials are provided that demonstrate how this can be used, in combination with Google Cloud command-line tools, to enhance case data with e.g. entity recognition, sentiment analysis, text classification, and translated document texts.
- The suggestions in the Identities tab can now be sorted by name and by item count.
- Added suppression of noisy values in some of the Content Analysis branches.
- Performance and stability improvements in skin tone analysis.

- Resolved the Insight tab failing to update its status in the Workflow section after the user ran OCR, Email Threading, etc.

OCR

- Resolved the error messages that could occur when one clicked the Stop button in the OCR progress dialog.
- Resolved a discrepancy between the amount of OCR candidates reported in the Insight tab's Workflow section and the actual number of items that get OCRed. This is because the OCR output is applied to all duplicates. The count would differ when OCRed images were embedded, as well as be present as loose files or attachments elsewhere in the case.
- Resolved the OCR dialog failing to cancel properly when in the middle of the validation phase.

Tasks

- Resolved an issue with tasks made with Intella 2.1 failing to load in 2.1.1.x.
- Improvements to make restoring annotations more robust.

Searching

- The Search button is now always enabled and, when no text has been entered, will return all items in the case.
- Added a Show Family search option. This new operation effectively combines the Show Parents and Show Children operations into a one-click operation, by determining for the selected item(s) the top-level parents and all their nested items. This also relates to the Families column in the Keywords tab and the Family Date field.
- The functionality for determining the top-level items now takes databases into account, so that these will not be the top-level items anymore. The Load File and Cellphone items are now captured into a single Forensic Containers category.
- Added a Features facet category that returns all top-level items.
- One can now upload multiple keyword, hash, and item ID lists at once.
- Improved tag names when using the Auto-tag function in the Keyword Lists facet.
- Reduced the logging of invalid keyword queries to a reasonable level.

Results

- Added a column that indicates whether an item is a top-level item.

Previewer

- Resolved missing inline images and attachments in iCloud emails.
- SMS and chat conversation items extracted from iTunes backups were lacking Next Day/Previous Day links and the Show Conversation search option. This has been fixed.

Tagging

- When adding a new tag, the Add Tags dialog lists any existing tags matching that text. This used to only list the tags whose name start with the entered text. Now it checks whether the tag contains the entered text anywhere in its name.

- The Add Tags dialog would not let users add a tag if all items in the set already had that tag. This check has been removed, as it did not take potential tag inheritance by family members and duplicates into account.
- Tagging events now show the full tag path, rather than only the tag name.
- Resolved quick tag keyboard shortcuts not working properly.
- Resolved an issue with the exporting of deep tag hierarchies in the Tags facet to a CSV file.

TEAM

- Improved the speed of populating the Table view.
- Improved the exporting speed.
- Improved the performance of the Show Parents and Show Children operations.
- Improved the handling of folder items recorded in an Intella Work Report (IWR) file.

Exporting – General

- Resolved not being able to export specific item types such as calendar items, reminders, notes, and devices, extracted from iCloud accounts or iTunes backups.
- A warning is now shown in the Export wizard when some evidence paths are missing.
- Exported conversation items now have a file extension.
- Resolved export issues caused by file name length limitations in MS Windows.

Exporting – CSV

- The hash character (#) can now be used as a delimiter.

Exporting – PST

- Resolved an issue with items failing to export to a PST file due to a quote character in the PST file path.

Exporting – Load Files

- Added “duplicate locations” and “duplicate custodians” fields. These report the locations and custodians of all duplicate items in the case, excluding the item itself.
- The encoding of a Relativity or Concordance load file is now configurable.

Upgrade Notes

Backwards compatibility – Intella 2.2 can directly open cases made with Intella 2.1.x, without any case conversions or other transformations.

When items in cases made with 2.1.x are exported to a separate case, the registered case size of the target case will be incremented with the size of the original case. This may be problematic for users with licenses that have a case size limitation. To resolve the inflated case size, the source case needs to be re-indexed before exporting items from it.

Intella 2.2 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 item data is converted, 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. Access to the original evidence files is not required for case conversion.

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 will 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.

Update notifications – The Intella update notification, shown in the menu bar when the user has the automatic update check enabled, now makes a distinction between regular version upgrades and patch upgrades.

Patch upgrades are released to fix urgent issues that cannot wait until the next release version. They are identified by the fourth digit in the version numbers. Users on an older release version (e.g. 2.1.1) always get to see the regular version announcement (e.g. about the 2.2 release). Users that are already on this release version get to see an announcement about a patched version if there is one (e.g. a 2.2.0.1 release), unless they are already using this patch version.

The download links in the support portal always point to the latest patch release.