Intella 2.7 Release Notes

Highlights

- Introducing **Intella Backpack**, a free companion product that can open **portable cases** generated by Intella Professional.
- **Identity improvements**, such as mass importing and exporting of identity data.
- Added exporting to the **AFF4-L logical image** format.

- A variety of indexing improvements related to **chat messages**, e.g. support for **Google Chat**.
- Added support for **EDRM MIH hashes**.
- Added **source filters**, letting one filter items based on file name or size.
- **2 to 5 times faster exporting** to PDF and load file formats.

Intella Backpack & Portable cases

- Intella Professional can now export items to a portable case. This new case format consists of a single encrypted file, holding a complete case consisting of the exported items. The file is password-protected, ensuring that only the intended recipient of the portable case can use it.
- The portable case can be opened in Intella Backpack. This new and free application allows users to review and search the items in the portable case.
- On the technical side, Intella Backpack is constructed as a portable application. This means that it can run without installation, and without requiring administrative rights. Just unzip the ZIP file and double-click IntellaBackpack.exe. For example, it is possible to run it straight from a USB memory stick.
- No license is required to run Intella Backpack. It will run freely and perpetually. Intella Backpack will be available to non-Vound customers as well.
- Exporting portable cases is subject to a usage-based license. Intella Professional 2.7 comes with 5 exports included in the standard license. Contact sales for extending this with additional exports.

Installer

- Resolved blurry desktop and taskbar icons when using high-resolution screens and display scaling.
- Resolved an issue with applications not uninstalling when uninstalled from Windows' Programs and Features / Apps and Features settings panel.
- Removed the "(x64)" suffix from all new firewall rules.

Case management

- When importing a case to the cases list, a check is done to see if a case with that ID (listed inside the case.xml file) already exists. When such a case is present, the user is asked whether the imported case should replace the existing case with the same ID, or whether it should be imported with a newly generated case ID.
- Improved the default memory settings for new cases on machines with 512 GB or more RAM.

Indexing – General

- Added support for generating EDRM Message Identification Hashes (MIH). This is a cross-platform and cross-vendor message hashing standard, making email hashes comparable and exchangeable between forensic and eDiscovery applications.
- Added a source option to skip storing the binary data of items larger than a specific size. This helps reduce the case folder size and the indexing time. By default, items larger than 250 MB are not stored in the case folder anymore.
- Add a source option for skipping items based on their file name. This can be used to suppress files based on a known file extension or on another fragment in their file name.
- Put a limit on the length of the stored and indexed raw data. This increases performance and improves stability, by reducing the risk of memory errors. An example is chat conversations spanning a long time range, where the bundled metadata of all included chat messages can result in very large data streams. When indexing metadata fields,

Phone Enquiries
+1 (888) 291-7201

Postal Address
10643 N Frank Lloyd Wright Blvd, Suite 101, Scottsdale, AZ 85259 U.S.A.

Email sales@vound-software.com
Sales Contacts
www.vound-software.com/partners

www.vound-software.com

Vound
AMERICA • ASIA • EUROPE

only the first 1 MB of text will be indexed. Only the first 5 MB of raw data will be stored. Warnings are added to the case logs when data is truncated. Items that exceed a limit are marked as Exception items with the type "Truncated".

- Resolved an issue with the exception report failing to be produced.
- Resolved an issue with the temporary folder failing to be cleared.
- Resolved an issue with Hangul HWPX documents showing an incorrect file name.
- Resolved an issue with incorrect creation dates extracted from an Adobe Photoshop PSD file.
- Stability improvements in the post-processing stage.
- Stability improvements when processing lots of small files over a network connection.
- Stability improvements when indexing damaged EDB files. This affects MS Exchange email databases, Windows Mail databases, and non-email EDB files.
- Harmless warnings stating "End of data reached" when processing PNG images and MP4 videos are now suppressed.
- Resolved an issue with incorrect crawler memory settings being reported in the case logs.

Indexing – Disk images

- Resolved an issue with processing of VHDX images created by the Kroll Artifact Parser and Extractor (KAPE).
- Resolved an issue with missing folders when processing Apple DMG images.
- Resolved an issue with processing Japanese folder names in FAT32 images.
- Stability improvements when indexing Apple DMG images.

Indexing – Email

- Improvements to the processing of PST containers:
  - The Conversation ID column is now populated for emails from PST containers.
  - Resolved an issue with missing emails due to incorrect MIME structures. These emails were not represented as an item, nor was anything logged.
- Improvements to the processing of Apple Mail containers:
  - Added support for recent Apple Mail versions.
  - Resolved several cases of missing attachments.
  - Stability improvements.
- Resolved an issue with the parsing of email headers with duplicate recipient headers, e.g. multiple CC headers, rather than a single header with a list of addresses.

Indexing – Chat messages

- The Google source has been extended with support for Google Chat.
- Improvements to the processing of Cellebrite UFDR and UFED XML reports:
  - Resolved an issue with chat messages not being indexed.

- Resolved an issue with a UFDR file being incorrectly classified and processed as a Slack data dump.
- Improvements to the processing of RSMF files:
  - Added full support for the RSMF 2.0 standard.
  - Performance improvements. Next to the speed improvement, this also significantly reduces the chance of time-outs on very large RSMF containers.
- Improvements to the processing of MS Teams PST files:
  - Resolved an issue with conversations not being split properly by month or year.
  - Resolved an issue with inconsistent participant information between conversations and reply threads nested within that conversation.
  - Resolved an issue with start and end dates being reversed for some messages.
  - Stability improvements.
- Improvements to the processing of Slack data exports:
  - Improvements to the processing of the original and edited message timestamps.
  - Improvements to the processing of Slack participant usernames.
  - Stability improvements.

Indexing – Load files

- Improved the load file integrity check that is performed when the user clicks on "Check for Errors". Additional item type checks are being performed.

Indexing – Cloud sources

- The Google source has been extended with support for Google Chat.
- When selecting an S3 bucket or Google Drive to acquire, one can now indicate which folder(s) need to be acquired.
- Resolved several authorization errors when accessing Google sources.
- Stability improvements for SharePoint acquisitions.
- Improved error logging when indexing Dropbox sources.

Indexing – Crawler scripts

- Resolved an issue with crawler scripts failing to modify items that lack an MD5 hash.
- Resolved an issue with the Visited URL and Size fields not being accessible for crawler scripts.

IntellaCmd

- Added support for the -keyID argument. This lets one specify the dongle or SL key to use.
- Added a -replaceSourcePaths argument. This lets one do a substring replace of all evidence paths of all sources in a case.
- Improved the lookup process for alternative licenses.
  - Intella Node licenses are now always preferred over Intella Professional licenses.
  - When the first applicable license already has all its seats consumed, it will switch to an alternative license with available seats, rather than giving up.

Phone Enquiries
+1 (888) 291-7201

Postal Address
10643 N Frank Lloyd Wright Blvd, Suite 101, Scottsdale, AZ 85259 U.S.A.

Email sales@vound-software.com
Sales Contacts
www.vound-software.com/partners

www.vound-software.com

Vound
AMERICA • ASIA • EUROPE

- Removed a false but misleading "Product license not found" error message. This was a byproduct of IntellaCmd simply trying out several alternative licenses.

- Improved memory usage of the case conversion process.

- Resolved an issue with Notes ID files not validating properly.

- Resolved an issue with case creation, where the main process memory setting of the specified case template was ignored.

- Resolved an issue where the system's temporary files folder was used, rather than the folder specified in the case settings. Also added some stability improvements related to the use of the temporary files folder.

- Resolved an issue with the -exportSourcesList operator failing to produce results when invoked on cases holding Slack data dumps.

Analysis

- Resolved an issue with selecting the built-in, hardcoded Content Analysis categories (Credit Card Numbers, Social Security Numbers, Phone Numbers) still enabling the Edit button. Clicking this button would yield an error.

- Scalability improvements to the "Generate duplicate custodians and locations" algorithm".

Full-text search

- Improvements to the searching of email addresses containing underscore characters.

- Improvements to the searching of acronyms.

Facets

- The Item ID Lists facet's import functionality has been extended to also support the importing of URI lists. This facilitates the exchange of item lists between one case and another case exported from that first case. The item IDs will differ between those cases, but the URIs are constant and can be relied upon to find those items in the other case.

- The Features > Exported category now also reflects items that were exported to a (portable) case.

- Resolved an issue with custodian information not appearing in a case converted from an earlier version. This affected the custodian information in the converted compound case itself, not the custodian information found in its converted sub-cases.

Identities

- Added importing of identities. Using a CSV file, identity data like names, organizations, email address and other communication aliases, etc. can be imported. This allows data on known identities to be utilized in a case.

- Added exporting of defined identities to a CSV file.

- The identity suggestions algorithm no longer suggests identities that have already been defined by the user.

Results

- UI improvements in the rounding of values such as byte counts.

- Quality improvements in thumbnail generation.

- Resolved an issue with the Hide Non-inclusive button not hiding all non-inclusive items in a compound case.

Previewer

- The rotation data in an image's EXIF data, if present, is now applied to the rendering of the image. This ensures that the image is rendering with the intended rotation.

- Resolved an issue with certain email SMTP headers failing to render in the Headers tab.

- Resolved an issue with flagging inconsistencies between messages in conversations and the underlying, nested items, due to internal parsing errors.

- Resolved an issue with the Previewer failing to render chat message attachments in a converted case.

- Resolved an issue with Slack-internal links not being followed properly when clicked in the Previewer.

Exporting – General

- Added exporting to the AFF4-L image format. This is a logical image format, similar to L01.

- Intella Professional has been extended with an option to export to a portable case. Portable cases are meant to be used by Intella Backpack. See the separate section on this new application for more details.

- Added an option to export item URI lists. These can be imported in the Item ID Lists facet. This facilitates the exchange of item lists between one case and another case exported from that first case. The item IDs will differ between those cases, but the URIs are constant and can be relied upon to find those items in the other case.

- Exporting errors are now reported to an Errors.csv file, separate from the regular export report that covers the successfully exported items. Optionally, this file can be converted to PDF, RTF and/or HTML, depending on the chosen main report format.

- Improvements to the suggested name of a new export set.

- Resolved an issue with inline attachments in Notes rich text emails being reported twice when exporting to EML or PST format.

- Resolved an issue with the "Edit Evidence Paths" hyperlink showing up in the export wizard of a compound case. Editing of evidence paths should be done in the corresponding sub-case. If evidence paths are determined as missing, a warning will now be shown in the compound case.

Exporting – PDF

- Speed improvements through the increased use of multi-threading. The improvement in total duration typically ranges between 2 to 5 times faster than the 2.6.1 version.

- The "For every email include" header in the PDF rendering options screen has been renamed to "For every communication include". This has been done because it applies to all communication types, not only emails.

Exporting – Load files

- The PDF-related improvements listed above also apply to the exporting to load files.
- Resolved an issue with comments being exported from one case to another through load file overlays. All comments would be squashed together, rather than kept as separate comments.
- Resolved a memory issue when using the "Export native chat content as PDF" option in the load file options.

Exporting – PST

- Resolved an issue with emails exported to a PST file lacking a Conversation Index field. This caused issues when attempting to perform email threading when the PST file was ingested in the Logikull platform.
- Resolved an issue with the automatic skipping of very large emails, done for stability and reliability reasons. An issue with the determination of the size of the email caused some emails to be skipped inadvertently.
- Resolved an issue with tasks with inconsistent timestamps failing to export to a PST.
- Resolved an issue with certain types of export errors not being reported in the export report.

Exporting – Relativity

- Adjustments to the firewall rules related to the direct export to Relativity.

Exporting – Case

- Compound cases now also support exporting items to a separate case.
- Case exporting now supports exporting Image Analysis, Email Threading and Near-Duplicates item data.
- Resolved an issue with exporting decrypted items to a separate case. Decrypted items that could be opened in their native format in the original case, would fail to open in the case that it was exported to.
- Resolved an issue with Skin Tone Analysis results not carrying over to the target case.

Intella Viewer

- Resolved items failing to render when opened in a Previewer, in a remote case shared by Intella Connect or Intella Investigator. In one case this affected MS Teams chat messages. In another case this affected tagged items in a compound case.

Retiring functionalities

Intella Viewer – In a future release, Intella Viewer's ability to connect to a case shared by Intella Connect or Intella Investigator will be removed. Intella Connect and Intella Investigator will be able to deliver those functionalities entirely via the browser.

Microsoft SharePoint – The 2.7 version will be the last version to support local, on-premises SharePoint instances. Cloud-based SharePoint instances are not affected by this change, as they can be retrieved using the M365 source type.

Upgrade Notes

Intella versions can be installed side-by-side. There is no requirement to uninstall old versions when installing an Intella version.

Case version 2.6.x – Intella 2.7 can open cases made with Intella 2.6.x. No case conversion is needed.

Due to a change in the underlying databases, results in the Image Categories and Detected Objects branches of the Image Analysis facet that were made with version 2.6 will not be visible when the case is opened with version 2.6.1 and later. This analysis will have to be repeated with the more recent version used.

Case versions 2.1.x to 2.5.x – Intella 2.7 can open cases made with Intella versions 2.1.x to 2.5.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 original 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 require sufficient disk space. As a rule of thumb, please reserve twice the amount of the evidence size for your case folder.

Other case versions – Cases made with Intella 2.0.x or older are not supported.

To open cases made with the 1.9.x and 2.0.x versions, please use Intella 2.5.1. This is the last version to support the 1.9.x and 2.0.x versions.

Cases made with beta versions are not supported and should be recreated.

Memory settings – The 2.7 version changes how case memory settings are stored. Prior to version 2.7, these settings were stored in both the case.xml and case.prefs files, for historical reasons. This is now only stored in the case.prefs file. Consequently, if the 2.7 version is used to alter the memory settings of a case made with an older version, the memory setting changes may not be picked up by older versions.

Software versions – Vound will provide technical support for one major past version. For this release that will mean the 2.6.x range of products. Vound always recommends that users upgrade to the latest version.