Intella INVESTIGATOR

Vound

Intella Investigator 2.6.1 Release Notes

Highlights

- Added support for acquiring and indexing **S3 buckets**.
- Added support for acquiring and indexing various **Google** services.
- Improved the presentation of **contacts, meetings, invites** and **phone calls**.
- Added an **Events view**, showing a timeline of events observed in the evidence data.
- Added a system for license add-ons, enabling larger amounts of active cases and reviewers.
- **Command-line support** has been extended with options for case conversion, custodians, type filters, various forms of exporting, and more.
- **Case conversion with IntellaCmd.exe no longer requires a license**, allowing the task of converting large amounts of cases to be spread across several machines.
- Added a **log management** page, for scanning and providing easy access to all logs on a server.
- **Authentication** enhancements for 2FA and SSO.

General

- Added a log management page to the Admin environment. This functionality scans all logs present in a Connect/ Investigator system: Investigator server logs, case logs and/or Node logs. The logs are checked against a list of common errors. Examples are errors related to file system permissions, disk space use, memory settings, etc. The user can download the logs from this page, removing the need to have file system-level access to various servers to obtain these logs.
- Windows Server 2022 is now listed as a supported OS.
- Resolved an issue with character encoding handling, which resulted in characters being displayed incorrectly.
- Resolved an issue with the temp folder setting sometimes not being used for certain tasks.
- Resolved an issue with file sizes being rounded incorrectly in several places.
- Various styling improvements.

Security

- Resolved a cross-site scripting vulnerability in the Tags facet.
- Resolved a redirection vulnerability in the Login page.
- Several library updates triggered by vulnerability analysis.

Licensing

- Added a modular licensing system for enabling more active cases and active reviewers on an Investigator server.

Authentication

- Added the ability to enforce the use of 2FA upon all users.
- Added a validator and troubleshooter for SSO setups.

Case management

- Suppressed a harmless error on case lock files when converting a case to the 2.6.x format.
- Resolved an error that occurred when importing certain case templates.
- Resolved several errors with case conversion failing to convert the geolocation database.

Compound cases

- A compound case's Custodian facet now shows a unified list of all custodians present in its sub-cases.
- Compound cases can now be converted fully automatically. In the 2.6 version, several manual steps were required to convert the compound case and all its sub-cases.
- Several enhancements in command-line processing involving compound cases. See the "Command-line support" section for more information.

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

- Resolved an issue with saved searches containing tags not loading properly in a compound case.
- Resolved an issue with the duplicate counts and the results of the Show Duplicates operation being too high in compound cases, due to items not being deduplicated across sub-cases.

Sources

- Resolved an issue where a source's type filter configuration defined in a Connect/Investigator source would show up inverted when viewed in the Intella desktop application.
- Added support for adding W4 cases made with W4 version 1.1.5.
- Resolved an issue with the "Analyze paragraphs" setting not allowing to be turned off.

Indexing – General

- Resolved an issue with DestList entries in a jump list not being extracted properly.
- Resolved an issue with all sources being marked as having an error after re-indexing, when only a subset of sources failed to index.

Indexing – Disk images

- The Select Folders sheet now shows volume labels when adding an APFS disk image. These were already extracted and shown in the Location facet; only the folder chooser was not showing them until now.
- Resolved an issue with missing volume labels when indexing ISO images.
- Resolved an issue with certain DMG images failing to process.
- Resolved an issue with certain APFS file systems failing to process.

Indexing – Email

- Added detection of MS Outlook IRM-protected emails (.rpmsg files).
- Resolved stability issues when indexing EDB files.

Indexing – Chat messages

- Resolved an issue with chat messages without a protocol that would fail to index.
- Resolved an issue with the chronological ordering of edited Slack messages.
- Resolved an issue with the Raw Data of certain chat messages lacking the full list of recipients.
- Resolved an issue with non-existing folders appearing in the Location facet when indexing a Slack Enterprise Grid export.

Indexing – Cloud

- Added support for indexing Amazon AWS S3 buckets.
- Elevated the Gmail source to become a Google source. Currently supported Google (Workspace) services are Gmail, Drive, Calendar, Tasks and Contacts. Future versions will extend this to a broader set of Google services.
- Resolved an issue with iCloud sources producing cookie validation failures.
- The "Connect to iCloud" page now uses a masked password field, obscuring the entered password.

Indexing – Crawler scripts

- Crawler scripts can now check whether an item passed to the script is a top-level item or a nested item. Examples of top-level items are the files in a file system folder and the emails in an Outlook PST file. Examples of nested items are images embedded in a document and files attached to an email. This family information allows for more fine-grained filtering of items, where the parent role is often crucial. For more information, see the GitHub page on crawler scripting: https://github.com/vound-software/intella-crawler-scripts.
- Resolved an issue when multiple sources with a crawler script were re-indexed. Re-indexing could give a fatal error when the second source was re-indexed.

Command-line support

- IntellaCmd.exe is now also installed when installing Intella Investigator/Connect. Previously, this was only installed with Intella and Intella Node.
- IntellaCmd.exe will now revert to looking for a Connect or Investigator license, when a Node or Professional license cannot be found.
- Added support for case conversion to IntellaCmd. Previously this could only be done by Intella.exe or interactively.
- No license is needed to run IntellaCmd.exe for case conversion.
- Added support for creating a compound case.
- Added support for specifying a case template when creating a new case.
- Added the ability to set a crawling script in a source configuration.
- Added the ability to set the custodian when adding evidence items to a case.
- Added the ability to include or exclude a list of item types during indexing. Depending on the filtering mode used, all items with a MIME type on, or not on the list are skipped.
- Added the ability to install a hash list through a command-line call, and to specify its use as part of a source definition.
- Added the ability to add various forms of data in bulk: source paths, BitLocker recovery files, password lists, email certificates and Notes ID files.
- The "-importText" option can now also be used on a compound case.
- Added the ability to export items using an export template. This change allows all export types to be automated through command-line arguments.
- The events.log file, containing a record of all actions taken place in a case, can now be exported to a CSV file through command-line arguments.

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

- Added a "-listAllTimezones" argument, which list all timezones that can be used in Intella(Cmd).exe invocations.
- Added options for exporting the exception report and a separate "fatal errors" file. These reports reduce the chance of critical errors being overlooked.
- Resolved an issue with the "-exportSourceList" command not exporting all chat-related settings of a source.
- Resolved an issue with paths failing to work due to the presence of a backslash character at the end of a quoted string, which resulted in the backslash being interpreted as the start of a character escape sequence.

Searching

- Improved the Image Analysis facet user interface and underlying database. Thresholds for image and object categories can now be altered directly inside the Image Analysis facet, instead of via the Preferences window. Changing the threshold immediately alters the facet counts, without requiring lengthy database updates.
- Resolved an issue with Boolean queries involving single term phrase queries with leading and trailing wildcards not producing adequate results.

Results

- Added an Events view. This view shows the timestamps of results as a list of events sorted chronologically. Selecting an event will show the details of the item corresponding with that event in a preview panel.
- Resolved an issue with the Select All and Invert Selection buttons in the table's right-click menu not working.
- Resolved an issue with the item counts in the facets and the Searches list not considering that certain items may be hidden due to the use of the "Cannot see items tagged with ..." permission. While those items were not uncovered, the item counts shown in those places were incorrect.
- Resolved an issue with the table column widths being restored to their default widths when the table is updated.

Analysis

- Image Analysis and Object Detection have been extended to support more image formats, e.g. iOS HEIC images. As a rule of thumb, when an image can be displayed in the application, it can now also be subjected to Image Analysis and Object Detection.
- The algorithm for suggesting Identities now ignores accounts named "admin" or "administrator".

Previewer

- Enhanced the presentation of items representing contacts, meetings, invites and phone calls. The Contents tab now shows the relevant properties of these items in an appropriately formatted list, making the information easier to review.
- Enhanced the rendering of images in the Previewer.
- Added a slider for the object detection threshold. This allows the user to control whether all detected objects are highlighted or only the highest scoring objects.
- Resolved an issue where hidden slides, speaker notes and comments of a PowerPoint file were not rendered, when viewed in the native rendering.

Exporting – General

- Resolved an issue with export packages larger than 2 GB failing to download.

Exporting – PDF

- The enhancements for rendering contacts, meetings, invites and phone calls listed in the Previewer section also apply to the PDF export of these items.
- Resolved an issue with some PDF items failing to export to PDF.
- Resolved an issue with some JPG images failing to export to PDF.
- Resolved an issue with chat messages and conversations failing to export when they include corrupt embedded images.
- Resolved an issue where hidden slides, speaker notes and comments of a PowerPoint were not rendered, when exported to native rendering.
- The "Prefer HTML over plain text" option for email exporting is now selected by default.

Exporting – PST

- Resolved an issue with emails with LDAP-style addresses failing to export to PST.
- Resolved an issue with emails with tens of thousands of recipients failing to export.

Exporting – Load file

- All PDF-related export changes apply to load files as well.

Exporting – Report

- Resolved an issue with the Next button on the "Report – Title Page" sheet staying disabled.

Export – Case

- Resolved an issue with tags that are not assigned to any items, but are present in the Tags facet, not being exported to the target case.

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

Upgrade Notes

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

Case version 2.6 – Intella Investigator 2.6.1 can open cases made with the 2.6 version of Intella, Intella Connect and Intella Investigator. 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. This analysis will have to be repeated with version 2.6.1.

Case versions 2.1.x to 2.5.x – Intella Investigator 2.6.1 can open cases made with 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 version 2.0.x or older are not supported.

To open cases made with the 1.9.x and 2.0.x versions, please use version 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.

Software versions – Vound will provide technical support for one major past version. For this release that will mean the 2.5.x range of products. Vound always recommends that users upgrade to the latest version.

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