DETEGO GLOBAL

DETEGO

2026 R2

RELEASE NOTES

ENHANCEMENTS TO DETEGO ANALYSE AI+

1. Rapidly Identify Malware and Suspicious Files Using YARA-Based Scanning

This release introduces YARA-based scanning, helping investigators quickly identify files, memory artefacts, and backup data that may contain malware, malicious code, or indicators of compromise. By automatically scanning digital evidence against custom YARA rules, investigators can swiftly surface suspicious content for further examination, reducing manual review and accelerating threat-focused investigations.

YARA uses flexible rule-based pattern matching to detect known malware families, suspicious behaviours, and custom indicators across a wide range of evidence types. This enables investigators to identify potentially malicious artefacts earlier in the investigative process and focus their efforts on the most relevant evidence.

A new YARA Rules configuration page has been added to Detego Analyse AI+, providing a central location to manage rule libraries. Investigators can add, upload, rename, export, and organise YARA rules, while a built-in preview function allows rule content to be reviewed without leaving the platform.

During a YARA Scan, Detego automatically evaluates files within an exhibit or filtered dataset against the configured rules. Any matches are automatically tagged, enabling investigators to quickly locate suspicious files, prioritise analysis, and uncover evidence of malware activity, compromise, or unauthorised software execution.

2. Quickly Pinpoint Valuable Intelligence Hidden Within Document Metadata

This release introduces a new Document Metadata Extractor analytic job, helping investigators automatically extract and index metadata from all supported document evidence types such as PDF, Excel, and Word (excluding plain text documents). By making document metadata searchable within Detego Analyse AI+, investigators can rapidly uncover authorship information, document properties, and creation or modification details that may support attribution, timeline analysis, and evidential review.

Extracted metadata is automatically indexed and made available through the Document Metadata section of the OmniViewer's Text Index tab. For more targeted workflows, the job can be configured to extract metadata from specific document types using the advanced job queue builder.

3. Easily Filter Evidence Based on Exif Data

The Exif Data filter has been enhanced to help investigators rapidly identify relevant images and videos based on embedded Exif metadata. Investigators can now return items that either match or do not match a specified Exif value, enabling faster filtering of large datasets and more efficient identification of media linked to specific cameras, devices, or metadata attributes.

4. Find Relevant Evidence Beyond Keyword Searching

This release introduces Semantic Text Search, helping investigators find relevant evidence based on meaning, context, and sentiment rather than relying solely on exact keyword matches. By understanding the intent behind a search, Detego Analyse AI+ can surface relevant chats, emails, documents, and other text-based evidence even when the exact search terms do not appear within the content.

This capability can help investigators uncover critical evidence more quickly across a wide range of investigations, including cybercrime, fraud, child exploitation, intelligence, and corporate investigations. By identifying semantically related concepts and terminology, it can help surface relevant information even when alternative wording, commonly used slang terms, or indirect language is used.

For example:

- A search for "aggressive messages" may identify threatening or hostile communications.
- A search for "COVID PPE clothing" may return documents relating to coronavirus face shields or protective equipment.
- A search for "pensions and investments" may surface financial planning and investment-related documents.

Semantic Text Search can be enabled through the Text Indexing job and accessed via the new Search Options window within the web interface. Future releases will extend this capability to support multilingual semantic searching.

5. Improve Platform Performance and Simplify Deployment by Migrating to SQLite

This version of Detego converts the core database from MySQL to SQLite format. This is a one-time migration that occurs automatically when 2026 R2 is installed for the first time.

Important: This migration can only be performed on Detego version 4.16 or later. Installations running versions prior to 4.16 must be upgraded to a compatible version before installing 2026 R2. Upgrading to 2026 R1 first is strongly recommended before proceeding with this version.

6. Benefit From Brazilian Portuguese Language Support

This release adds Brazilian Portuguese localisation to both Detego Analyse AI+ and Detego Field, helping investigators and forensic teams work in their preferred language. This enhancement further strengthens Detego's support for global investigative and forensic teams and builds on existing localisations, including German, French, Italian, Swedish, Spanish, Japanese, and Arabic.

NEW FEATURES FOR WEB-BASED DETEGO ANALYSE AI+

7. Easily Search and Filter Evidence Geographically With the Map View

This release introduces a dedicated Map View within the Evidence Browser, helping investigators quickly visualise, explore, and filter GPS coordinate evidence on an interactive map. By plotting location data geographically, investigators can more easily identify areas of interest, uncover location-based patterns, and focus analysis on relevant regions.

GPS coordinates are automatically displayed as markers and clusters, enabling investigators to navigate large volumes of location data with ease. Selecting a marker reveals associated evidence, including item details, coordinates, and thumbnails, while direct integration with the OmniViewer provides rapid access to underlying evidence.

Investigators can also filter evidence geographically by selecting specific regions on the map, helping narrow datasets to relevant locations and accelerate location-based investigations.

The Map View uses the mapping provider configured within Detego, supporting both OpenStreetMap and offline maps.

8. Quickly Validate Location-Based Evidence With the New MAP Tab

This release introduces a new MAP tab within the OmniViewer, helping investigators quickly visualise the exact location associated with an evidence item without leaving their current workflow.

For GPS Coordinate items, the MAP tab is selected by default and displays the item's location on an interactive map alongside its associated properties, providing immediate geographical context

for location-based evidence.

For picture and camera files containing EXIF GPS metadata, the MAP tab is available alongside the standard PICTURE tab, helping investigators view both the image and its capture location without leaving the OmniViewer. For these files, the PICTURE tab remains the default view; the MAP tab is available but not selected automatically.

9. Configure Your Mapping Provider for Online and Offline Environments

A new Mapping Provider setting under the Configuration panel enables users to select which map provider is used for displaying location data across the application. Two providers are currently supported:

- OpenStreetMap: the default option, tile-based and requiring an active internet connection.
- Offline Maps: for environments without internet access, requiring the Detego or MSAB offline mapping packages to be installed via the Installation Manager.

On the desktop platform, selecting Offline Maps also exposes a Custom Offline Maps Folder option, allowing an alternative directory for offline map files to be specified in addition to the default path.

Note: Offline Maps requires the relevant mapping packages to be installed separately. Contact support@detegoglobal.com for assistance.

10. Streamline Evidence Searching With the New Search Options Window

This release introduces a new Search Options window, providing investigators with a central location to configure and manage search settings within Detego Analyse AI+. Accessible via the cog icon next to the search box, the Search Options window makes advanced search capabilities easier to access, helping investigators quickly switch between search methods and refine results to uncover relevant evidence easily.

The Search Options window supports:

- Standard Text Search for keyword-based searching using the Lucene index.
- Text Semantic Search for finding evidence based on meaning, context, and sentiment rather than matching keywords.
- Visual Semantic Search for finding relevant images based on their visual content following the Semantic Visual Indexer job.

A semantic similarity threshold can be adjusted for broader or stricter result sets. Investigators can also search using a picture file to return visually similar images from the exhibit. A search modes bar displays the currently active modes and provides quick access to edit settings via an Edit Search Settings button.

If the required job has not been run, a prompt is shown to initiate it directly. If the AI pack is not

installed, a message is displayed to flag this to the user.

11. Easily Search for Visually Similar Images Using a Picture

This release introduces Search Using Picture in the web interface, helping investigators quickly identify visually similar images within an exhibit. Accessible through the cog button next to the search box, investigators can select a picture and return visually similar images from within the exhibit.

A new Search for Similar context menu option on picture items enacts the same search using the selected picture directly, without opening the search configuration window.

12. Swiftly Generate PDF Reports From the Evidence Browser

A new Export to PDF option in the Action Items context menu provides a fast, one-click path to generate a structured PDF report from the current Evidence Browser view, without opening the Advanced Export dialog.

The export runs as a background job, allowing investigators to continue working while the report is compiled. A progress spinner is displayed on the Action Items button during processing, and a success notification is shown on completion. On the desktop platform, the output folder opens automatically in Windows Explorer.

The output includes the PDF report alongside a Logical Data subfolder containing copies of the physical files referenced within the report.

13. Produce Targeted Reports Based on Active Filters

When one or more filters are active in the Evidence Browser: such as file type, tag, keyword match, or evidence type: any report generated via Export to PDF or Advanced Export/Report is automatically scoped to reflect only the matching evidence items.

This allows investigators to produce precise, investigation-focused reports without manual selection, with the filtered scope confirmed by the item count and the resulting report structure on completion.

14. Export Comprehensive Reports with Enhanced Advanced Export Options

The Advanced Export dialog has been significantly enhanced. The dialog now uses a collapsible section layout, with each of the four main sections – Name & Location, What to Export, Advanced Settings, and Privacy & Redaction – independently expandable or collapsible for a cleaner, more focused interface.

The Formatted Report export type is now fully functional within the Advanced Export flow, supporting output in PDF, DOCX, and HTML formats. Multiple formats can be selected simultaneously to produce a combined export in a single job. Items within formatted reports include clickable embedded links to their corresponding physical files in the Logical Data folder,

allowing investigators to access original artefacts directly from the report.

New Formatted Report Options in the Advanced Settings section provide control over:

- Embedding thumbnails of picture-type artefacts.
- Creating separate sections for each keyword or regex match found.
- Including supplementary exhibit metadata files.

Data Listings (JSON, CSV, XML, XLSX) and Formatted Report exports can be enabled simultaneously in the same job. All existing Privacy & Redaction settings continue to apply to both export types. Users can also now customise the export file name within Advanced Export Settings, with validation applied for forbidden characters and minimum input length.

15. View Email Threads and Browse Outlook Container Files in the OmniViewer

Email thread viewing is now supported within a dedicated Email tab in the OmniViewer, with support for common Outlook file types including .msg and .eml.

Users can also now browse the contents of Outlook container files such as PST and OST directly through the OmniViewer without any prior job being run. Contained attachments are visible within the view, with the ability to open attachments planned for a future release.

16. Run Text Translation Jobs Directly From the OmniViewer

Text translation jobs can now be initiated from within the Document and Text Index views in the OmniViewer, removing the need to navigate to the job queue. Once a translation job has been run, the translated text is available to view directly within the Text Index View.

Note: This requires the text analysis language classification job to have been run in Detego Analyse AI+ first, and the text indexing job to have been run prior to that (which can be initiated from within the web interface).

17. Explore Archive and Parent-Child File Relationships via the Context Menu

This release introduces new context menu options that help investigators more easily explore relationships between archive files and their contents.

When reviewing a file extracted from an archive, investigators can use the Show Parent Archive File option to jump directly to the source archive. Likewise, when reviewing an archive file, the Show Contained Files option provides immediate access to all files extracted from it.

These enhancements make it easier to trace file origins, understand archive contents, and

navigate complex evidence sets.

18. View Items in Timeline Context From the Evidence Browser

A new View in Timeline context menu option enables investigators to jump directly to a selected item in the Timeline View, displayed in month view by the chosen date property. The item is pre-selected, enabling immediate contextual review alongside other items sharing the same date.

19. Configure Bounding Box Display and Other Settings From a New Configuration Window

A new Configuration window, accessed via the cog button at the top right of the page, centralises application settings. The initial release includes a Draw Bounding Boxes toggle, controlling whether detected objects are overlaid with bounding boxes in the image view of the OmniViewer following an object detection job. Further settings will be added to this window in future releases.

20. Review Conversations More Easily With an Enhanced Message Layout

The chat message view has been redesigned to provide a more compact and streamlined experience. Timestamps now appear beneath message bubbles, spacing and padding have been reduced throughout, and the panel layout has been adjusted to provide more space for the message groups panel.

A new Scroll to Top icon has also been added, making it easier to navigate lengthy conversations.

21. Generate Chat Reports Directly From the Evidence Browser

Users can now generate a PDF report for a message group directly from the Evidence Browser when viewing messages, eliminating the need to navigate away from their current workflow. Report generation progress is tracked via the standard job progress widget, consistent with existing export behaviour.

22. Play Media with Enhanced Controls and Multiple Subtitle Track Support

The media player has been enhanced to support caption and subtitle tracks, including media containing multiple subtitle tracks. Additional playback controls include a playback speed selector, a loop playback option, and general usability improvements across the player interface.

23. Use the Evidence Browser in Your Preferred Language

The web-based Evidence Browser now supports switching between all languages available in Detego Analyse AI+, ensuring a consistent localised experience across the platform. Investigators can now pick from Bazilian Portuguese, German, French, Italian, Swedish, Spanish, Japanese, and

Arabic.

24. Benefit From Improved Client-Side Diagnostics with Centralised JavaScript Logging

A centralised logging bridge has been introduced that allows any client-side JavaScript to write structured log entries directly into the server-side logging pipeline. This means client-side events and errors are now captured alongside server-side logs in the standard Detego web log files, simplifying diagnostics and support without requiring custom instrumentation for each component.

UI Upgrades and Improvements to Web-Based Detego Analyse AI+

25. Access Richer Item Detail With the Artefact Preview Flyout Panel

A new flyout info popup displays more detailed information about exhibit items on mouse hover, providing quick access to key metadata without navigating away from the current view. Investigators can also add and remove tags directly from the flyout panel, streamlining tagging workflows without the need to open a separate view.

26. Easily Browse Folder Structure With the New Folder View Panel

A Folder View panel has been added to the Filters panel, with toggle buttons allowing users to switch between the filter-based and folder-based navigation views within the same panel.

27. View Device Information and System Reports in the Exhibit Contents Panel

The Device Information content category has been added to the Exhibit Contents panel. Within this category, the System Information Report provides a structured summary of device system data, accessible directly from the panel without additional navigation.

28. Browse Extracted Data by Type in the Exhibit Contents Panel

An Extracted Data category has been added to the Exhibit Contents panel, with sub-category options for each type of extracted data: such as Video Frames and System Files: enabling more targeted navigation within large exhibits.

29. Navigate the Evidence Browser Banner More Easily

The small Exhibit Browser link in Detego Analyse AI+ has been replaced with a more prominent, fully clickable banner. The entire banner acts as a navigation link, with the exception of the feedback email address, which opens the feedback and bug report window directly.

ENHANCEMENTS TO DETEGO FIELD

1. Easily Extract Individual Encrypted Partitions Without Imaging the Full Disk

Detego Field can now extract individual encrypted partitions, including those protected by BitLocker, without requiring the entire physical disk to be acquired. This enables investigators to access encrypted data more quickly, reduce acquisition times, and focus on relevant evidence without capturing unnecessary data from the rest of the drive.

To access a locked partition, connect the Field device (and any collectors) to a Detego Analyse AI+ installation and select the option to import a physical image. Detego Analyse AI+ will prompt for the BitLocker password, after which the partition data will be available for processing and analysis.

2. Benefit From an Updated BitLocker Forensic Image Workflow

The workflow for extracting BitLocker-encrypted forensic images has been updated for installations where Passware is present. Where the BitLocker encryption type is supported by Detego's built-in decryption and the supplied password can unlock all encrypted partitions, the BitLocker Decryptor job is used automatically. The password entered in the encrypted image password dialog is passed directly to the job queue, reducing manual intervention and simplifying the workflow.

The BitLocker Decryptor produces a new image from the original with encrypted partitions unlocked, and copies any additional partitions detected in the source image to the output. Logical Extraction and Carving jobs in the queue then target the output of the BitLocker Decryptor job. Where the encryption type is not supported by Detego's built-in decryption, Passware is used as a fallback.

3. Perform Logical Extractions From Ballistic APFS Forensic Images on macOS

Logical extraction of Ballistic (E01) APFS forensic images acquired from non-chipped macOS targets is now supported alongside the existing DD format. This feature applies to unencrypted APFS images only. FileVault encryption must be disabled prior to acquisition.

For unencrypted macOS APFS images, no password is required and the macOS Login tab will be unavailable when configuring the logical extraction job. A dedicated flowchart has been added to guide users through the supported logical extraction workflow for non-encrypted E01 APFS images acquired from non-chipped hardware.

4. Parse Windows Search Databases for Richer Windows 11 Artefacts

Field now parses Windows Search databases on Windows 11 targets to extract a broader range of forensic artefacts. This includes indexed files with complete paths, browser history, and application activity data, extending investigative coverage for modern Windows 11 deployments.