

DETEGO

2026
R2 

TROUBLESHOOTING GUIDE

TROUBLESHOOTING GUIDE

1. Bounding Boxes Not Displayed for Symbol Detection Jobs

After running the Symbol Detection job, bounding boxes will not be displayed around detected symbols in the Evidence Browser because the Symbol Detection process uses advanced AI that does not generate bounding box overlays. Bounding boxes are a feature of the standard Object Detection job.

2. AI Generated Content Detector

Ensure the associated metadata is intact so that the AI Generated Image Detector can identify synthetic pictures and videos.

3. Remotely Issued Field Devices

The use of SSD drives connected via USB-to-SATA adapters is not recommended for Field Devices. In some cases, the serial number which is recorded in the Field Device license is the serial number of the adapter, rather than of the SSD. This may cause license violations if the Field Device is then connected using a *different* adapter.

4. Optical Discs

To ensure seamless data acquisition from optical discs (CDs and DVDs), we recommend utilising the Mounted Drive option instead of the Physical Disk option, as the latter may encounter challenges.

5. Date Range Acquisition

When applying the date and time range filter to a logical extraction job, inconsistencies in file counts may arise. Our engineering team is aware of this issue and is actively working towards a resolution.

6. Extracting Data From Encrypted Drives

To extract data from an encrypted drive (unlocked before extraction), use the **Acquire Connected Media > Mounted Drive** method instead of the Physical Disk method. The Physical Disk method may not yield the desired results. For BitLocker-encrypted drives, customers may acquire the encrypted data using **Acquire Connected Media > Physical Disk** and then decrypt later using the Physical Image Decrypter job.

7. Ballistic Imager

- Adding the compression option for a Ballistic Image may cause a temporary UI freeze before the extraction completes. Please give the UI a few seconds to refresh or turn off compression for Ballistic extractions.
- When performing a live extraction on a volume containing an unlocked BitLocker partition, targeting specific partitions rather than the entire volume is important. Avoid targeting the entire volume to ensure a focused extraction process.

8. Password Decrypting – File Viewing

- OpenOffice documents are not decrypted in Detego Analyse AI+ when using Passware. You can open the documents in the original application using the password extracted by the Passware Detector job.
- Legacy Microsoft Office documents (e.g., DOC, XLS, PPT) are decrypted but cannot be viewed within the OmniViewer. There are two possible resolutions for this: either use the method above or right-click the file, choose the 'Save Copy As' option, and save the decrypted file to your local drive for review.
- If a version of the Passware SDK older than the current version has been installed on the Analyse AI+ machine in the past, it may be necessary to remove temporary files created by those versions to allow encrypted file support to work correctly in Detego. Please contact support@detegoglobal.com for assistance.

9. Field Licensing

- We have substantially improved the speed of licensing hash lists to Field Devices. The licensing process for large hash lists, including those with over 150 million hashes, will be completed much faster than before. Even when password-protecting a hash list, the time overhead will be minimal.
- Detego Analyse AI+ will display a progress bar without the progress percentage while licensing a large hash list database. The process will still be completed.
- Please note that a maximum of 10 hash lists/databases can be loaded on a Field Device.
- When licensing Legacy Field for Windows 7, the Lime.exe dependency can get flagged by Windows Defender as a threat. To resolve this, add the Field Device to the Windows Defender exclusion list and then re-license it.

10. CFID

We currently only support the Encase 4, 5, and 6 image types for EWF images in CFID. DD images **MUST** also be created without compression. Please ensure you have configured the image type on your CFID device before creating and importing the image into Detego Analyse AI+.

11. Detego Field

- Only devices with a valid serial number and at least 2GB of storage can be licensed. Some budget USB devices do not have serial numbers, and Detego Analyse AI+ may not detect them (we also do not advocate using cheap USB devices from a longevity, heat management, and reliability perspective).
- Only devices with a maximum 2TB storage can be used for a Boot Device. If you wish to use a larger storage device for Field extractions, please create a separate Boot Device on a smaller USB for example.
- While most file types are viewable in Disk Inspector and View Extracted Data, some document/file types are not currently supported.
- Please note that Live BitLocker Decryption is currently in beta, and it may take considerable time to search for BitLocker recovery files in unencrypted drives and match the recovery key format. We recommend allowing extra time for the search and matching process to complete.
- When extracting macOS devices with an M1 (Big Sur) / M2 (Monterey) chip, please allow a few minutes for Detego Field to initialise, count the files, and begin the extraction.
- Attempting to import a revoked Field Device may result in an error. Please import Field extractions before revoking.
- You may need to refresh the Field Device list to see Connected/Disconnected devices when revoking Field Devices.
- Windows 7 machines do not recognise multiple partitions on SSDs. Please use an SSD with a single partition, a USB Field Device or a standalone Boot Device to avoid this.
- It is not currently possible to target mounted network drives using Detego Field.
- To ensure the integrity of your extractions, please import and revoke version 4.10.3 Field licenses before upgrading to version 4.11. Once on version 4.11, re-license your Field Devices.
- Photorec treats e-book files as archives and does not extract them if the carving job was configured to extract 'E-Book' only. In some cases, Photorec can identify an e-book file as a document. To ensure e-books are recovered, set the option to 'All Files' or 'Archive' on the carve job options.

- The RAM size is limited in the Detego Boot Environment so performing hash-matching using a large dataset (10GB and above, including the safe hash files, e.g., NSRL) may significantly slow down performance.
- On a few occasions, Windows Defender blocks some Detego Field .dll file dependencies; in that case, restart Detego Field with system administrator privileges and try again. If the issue persists, please re-license a fresh Detego Field.
- iMac target machines configured with Apple's Fusion Drive technology are not currently supported as acquisition targets in Detego Field. The Fusion Drive, which combines a traditional hard disk drive (HDD) with a solid-state drive (SSD) into a single logical volume, presents compatibility challenges that prevent Detego Field from successfully reading the internal storage. As a result, forensic acquisitions cannot be performed on these devices using this tool.
- Detego Media Acquisition supports logical DD (raw) forensic image extractions from non-chipped macOS targets. File carving, as well as logical extraction for E01 and Ex01 formatted APFS forensic images acquired from macOS targets, are not yet supported.
- Detego Media Acquisition may recover fewer files during carving when processing Ex01 forensic images compared to E01 or DD formats. For optimal results, it is recommended to convert Ex01 images to E01 or DD format before running carve jobs.
- The Boot Environment does not currently support RAID mode as the necessary RAID drivers are not included. Therefore, if the system is configured with the Storage-SATA/NVMe controller set to RAID mode, the internal drives cannot be mounted for some target machines.
- When running a Decryption job before a logical acquisition job on BitLocker-encrypted external media, the decryption process may become unresponsive or not complete successfully. Where the BitLocker recovery key or password is available, it is recommended to acquire the encrypted image and perform decryption within Detego Analyse AI+.

12. Storage Volumes

- If additional storage volumes are present within Detego, ensure they are unloaded/ejected correctly; this will maximise case/exhibit integrity.
- Some computers may put external adapters/hubs into low power mode if the device goes into sleep mode; configure your device to 'Always Stay Awake'.
- We advise using whole disk volumes as storage devices rather than partitioned volumes.

13. Antivirus

If you have issues with antivirus and your Detego installation or licensing Field Devices, contact support@detegoglobal.com for guidance.

14. Software Licensing

We recommend having Windows set to 'Set Time Automatically' to prevent 'License Blocking' issues caused by Detego's time/date change detection.

15. Detego Boot Environment

When using Field for Boot, the best practice is waiting for Detego Field to start automatically. This will ensure all files are loaded and the Field Device is ready.

16. Keyword Matching

For maximum file type support, we recommend running the keyword matching job *after* completing the logical extraction, rather than during it.

17. UFDR

Very few specific artefacts on the latest version of UFDR may be unsupported for import.

18. UI Refresh

You may need to click on the refresh button above the case list to update the cases in our system.

19. Hash List Import

In extremely rare circumstances (usually the result of a previous unsuccessful attempt), attempting to import a hash list from a .dhd file may immediately produce an error.

The workaround for this is:

- Browse to C:\ProgramData\Detego\Hashlists in Windows Explorer.
- Find the file with the same name as the one you are trying to import.
- Delete that file.
- Try the import again.

20. Evidence Time Zones

Detego may not be able to automatically determine the time zone offset from UTC that should be applied to the exhibit when extracting from some evidence sources. In this case, all exhibit timestamps will be reported relative to UTC.

The workaround is to specify the correct time zone in the Exhibit Metadata.

21. Localisation

While every effort has been made to ensure that localisation has been applied throughout the software, some English text may remain. We aim to address these instances in future service releases.

22. Intel Integrated GPU

On MSI spec machines, the integrated Intel GPU causes the Detego Analyse AI+ UI to freeze when running jobs. This is because the Intel Drivers distributed on MSI specs are older.

We recommend configuring the NVIDIA GPU (where available) as the primary GPU for Detego Analyse AI+.

Follow these steps to make the configuration change:

- Open the NVIDIA Control Panel application.
- Navigate to '3D Settings'.
- Select the 'Program Settings' tab.
- Section 1: Select a Program to Customise – Click the 'Add' button to add the 'Detego Analyse AI+' program in the drop-down menu.
- Section 2: Select the 'Preferred Graphics Processor' – set as 'High-Performance NVIDIA Processor.'
- Click the 'Apply' button.

23. Hash List Export

When exporting a hash list from Detego in plain text format, the output will be created as a CSV file with a separate row for each hash type (MD5/SHA1). When importing CSV hash lists back into Detego 4.12, you can only import one hash type at a time.

The workaround for this is either:

- Export the entire hash list as a DHD file and import that into other Detego instances, or
- Import the CSV file twice, selecting the MD5 column first and the SHA1 column second (or vice versa).

24. GMDSOFT MD-LIVE Import

- We are aware of an intermittent issue that may cause the importation of exhibits from MD-LIVE to complete unsuccessfully. This could leave an exhibit record in Detego which contains incomplete information.
- If you experience this issue during normal use, please report it to support@detegoglobal.com.

25. Rich Text Documents

In certain circumstances, when viewing Rich Text Format (RTF) documents in the OmniViewer, a progress indicator may appear in the middle of the viewer, even after the conversion is complete and the document is available.

26. Tag Deletion

- Tags applied to an item and subsequently deleted via the Configuration panel will not currently be removed from the active evidence browser and may display blank entries in the Tags sidebar.
- The workaround for this is to reload the evidence browser for the exhibit.

27. Media Indexing Jobs

After completion, the 'View Results' link displayed on a media indexing job may appear to open an empty evidence browser. The workaround is to open the exhibit directly from the case list instead.

28. Disk Inspector BitLocker Forensic Image/Physical Drive Support

Disk Inspector does not support inspecting BitLocker partitions in the exFAT file system. It only supports entire drive encryption for physical disks or images with BitLocker partitions.

29. Field macOS Live – Enabling Permissions

- After upgrading macOS to a newer version, some users may encounter the error 'Bad CPU type in executable' when attempting to run Detego Field. To fix this issue, installing Rosetta is recommended. You can do this by either using the following URL: <https://support.apple.com/en-gb/102527> or by running the command line (Terminal) `softwareupdate --install-rosetta`.
- In some cases, the user may need to change the default shell in the terminal by executing the following command: `chsh -s /bin/zsh`.

Versions of macOS released after Catalina (2019) require users to grant permission during the initial launch. If the user chooses to decline this option, the permission will remain disabled by default. However, the user can easily manually enable the permission in the Security and Privacy settings (please see **Annex 1**).

30. Video Transcription Subtitles

The in-built video player will always display transcription subtitles after running audio-to-text transcription for video files. If you need to view the video without subtitles, we recommend exporting the file and using an external video player.

31. Remote Acquisition – Remote Logical Extraction

The Detego Remote logical extraction job can be cancelled if the available disk space is exceeded during the process.

32. Physical License Keys

If you have a physical license key and install Detego Analyse AI+ without the license key connected, you may be presented with a login screen. Rebooting your machine will resolve this issue.

33. Document Mixed Language Translation

For documents containing multiple languages, use the advanced job configuration to enable the Detego Offline Translator to select target languages for translation. This will ensure accuracy in the automated language detection system.

34. Support for Reports Larger Than 2GB

To open a report larger than 2GB in the report viewer, use the available filters to generate multiple smaller reports.

35. Report Viewer Memory Issue on Instant Open and Close

Closing a report immediately after opening it in the Report Viewer may cause errors due to increased memory usage. We strongly recommend allowing the report to fully generate before closing the viewer. If the issue persists, restart the application.

36. OmniViewer New UI

An error message may appear after extended file previewing. To resolve this, disable the new user interface by toggling the switch within the window.

We are aware of several areas currently under review to optimise performance and usability. These include tag management, filtering, and the user interface.

Users may experience some limitations, such as duplicate tag creation, filter groups not saving, intermittent server reconnects, or keyword counts displaying total matches rather than file counts. We're also reviewing feedback related to UI responsiveness, redaction CSV exports, highlight scrolling, and interface alignment to ensure a smoother overall experience in upcoming updates.

37. Special Characters in List Names

We recommend avoiding special characters in list names (hash lists, keyword lists, face lists and job queues). You may be unable to rename or delete such lists if these special characters are used.

38. Single-file Mode Currently Unavailable for E01 and Ex01 Formats

While single-file mode is no longer supported when imaging to, or rebuilding extractions into, E01 or Ex01 formats, we recommend keeping the default 2GB chunk size when using these formats while we continue to improve stability.

39. RAW Image Display in Portable Viewer

If you are unable to view thumbnails of RAW camera files within OmniViewer through Portable Viewer, export them and open them in an external viewer.

40. Running Offline Translation on NVIDIA 5000 Series GPUs

Offline translation jobs may require you to switch to a different processing option (CPU or GPU) in the Detego system settings if your GPU is not yet supported (e.g. NVIDIA 5000 Series).

41. Screen Recordings

To ensure optimal performance of the screen recording feature in multi-monitor setups, we recommend that all monitors be set to their native resolution. If you need to adjust the size of text or icons, please modify the 'Scale' value within Display Properties instead of changing the resolution, as non-native configurations may produce unpredictable results.

Additionally, please note that the 'NO' and 'CANCEL' buttons on the navigation warning dialog currently perform the same function.

42. Physical Image Naming

To ensure a successful import via the Physical Image Importer, we recommend ensuring that filenames do not end in one or more spaces (e.g., image_01 .E01), as trailing spaces may prevent the ingestion job from completing successfully.

43. MSAB XRY Imports: Case Name and Path Length Requirements

Detego Analyse AI+ requires a valid case name when importing MSAB XRY extractions; imports with a blank case name are not supported. Additionally, importing iPhone extractions from MSAB XRY may not complete successfully due to path length limitations (255-character limit). To mitigate this, generate the .msabdetego file using MSAB artefacts with shorter file paths before importing into Detego Analyse AI+.

44. Missing Message Party Information in UFDR Imports

In some cases, message party details may be missing from imported UFDR files. Where this occurs, Detego Analyse AI+ will display <Missing Sender> or <Missing Recipient> in the relevant exhibits to indicate where sender or recipient information is absent.

45. Reports Tab: Windows Explorer Navigation

The 'Open Folder' button in the Reports tab may not always open Windows Explorer as expected. As a workaround, use the 'Copy Path' option on the success notification to copy the folder path and open it manually in Windows Explorer.

46. Windows 11 Smart App Control Installation Issue

When installing Detego on Windows 11 with Smart App Control enabled, installation issues may occur. To avoid this, disable Smart App Control via **Windows Security > App & Browser Control > Smart App Control Settings** before beginning the installation.

ANNEX 1

How to Allow Full Disk Access for Detego Field on macOS

To make sure **X** runs correctly from your USB drive, macOS requires that you grant it **Full Disk Access**. This gives the app permission to read and write files across your Mac.

Follow these steps:

1. Open System Settings (macOS Ventura / Sonoma / Sequoia)

- Click the **Apple menu** in the top-left corner (*Figure 1*).
- Select **System Settings**.

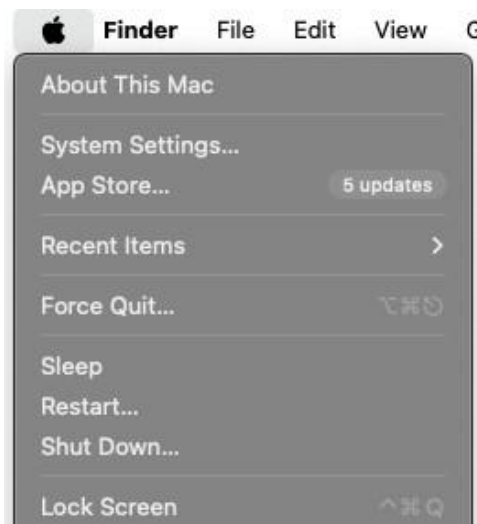


Figure 1

2. Go to Privacy & Security

- In the left sidebar, scroll down and click **Privacy & Security** (*Figure 2*).
- On the right, scroll until you find **Full Disk Access**.



Figure 2

3. Add Field Launcher to Full Disk Access

- Click the + button (Figure 3).
- In the file picker, navigate to your **USB drive** and select the **Run_mac** app (Figure 4).
- Click **Open**.
- Enter administrator password if prompted

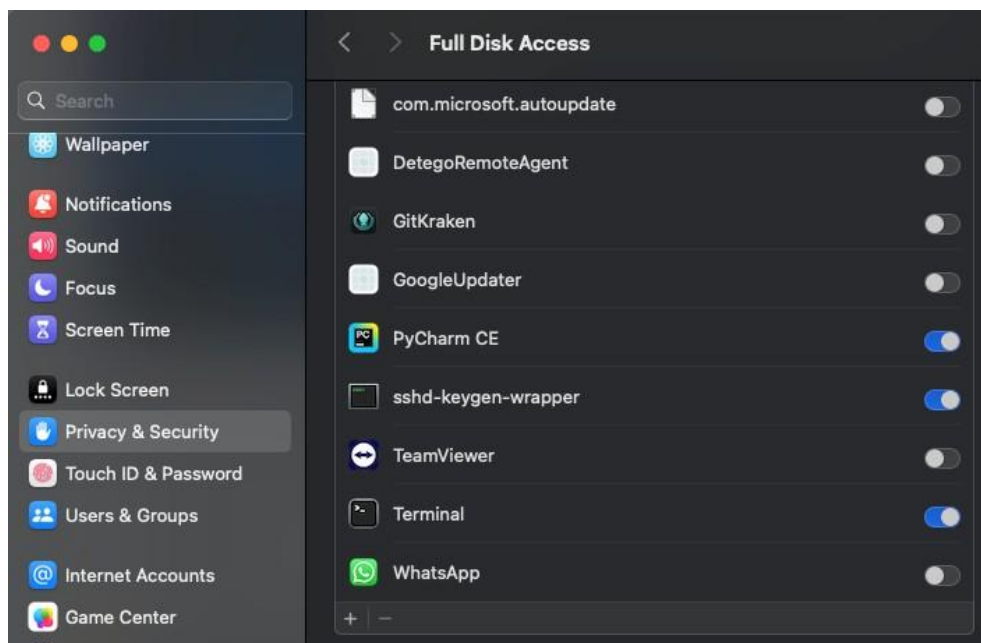


Figure 3

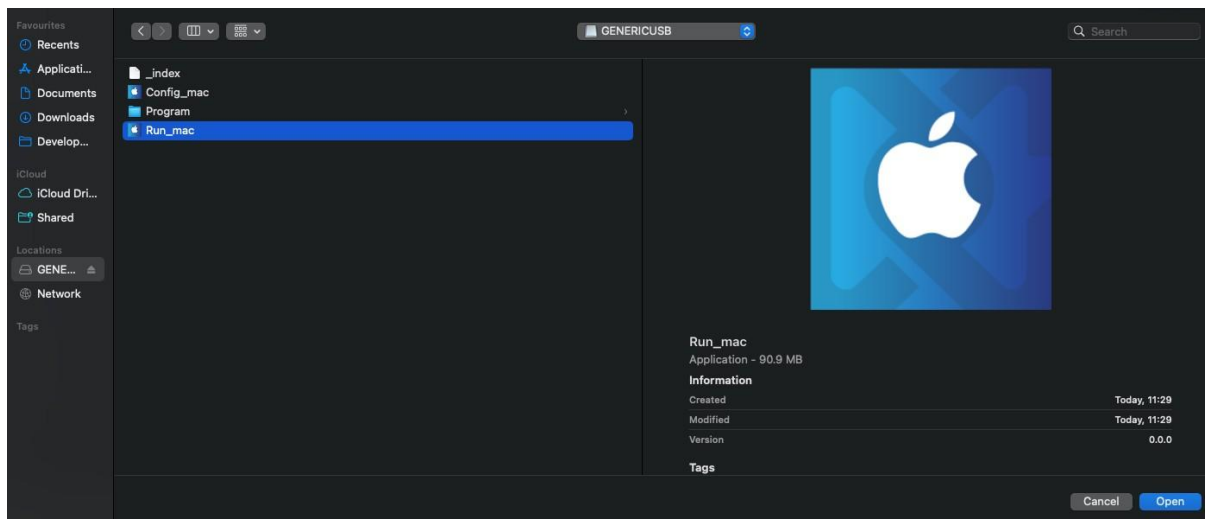


Figure 4

4. Add Field App to Full Disk Access

- Repeat the steps from section 3 but select the file titled 'field' at the path (Figure 5):

<PATH_TO_USB>/Program/Mac/field

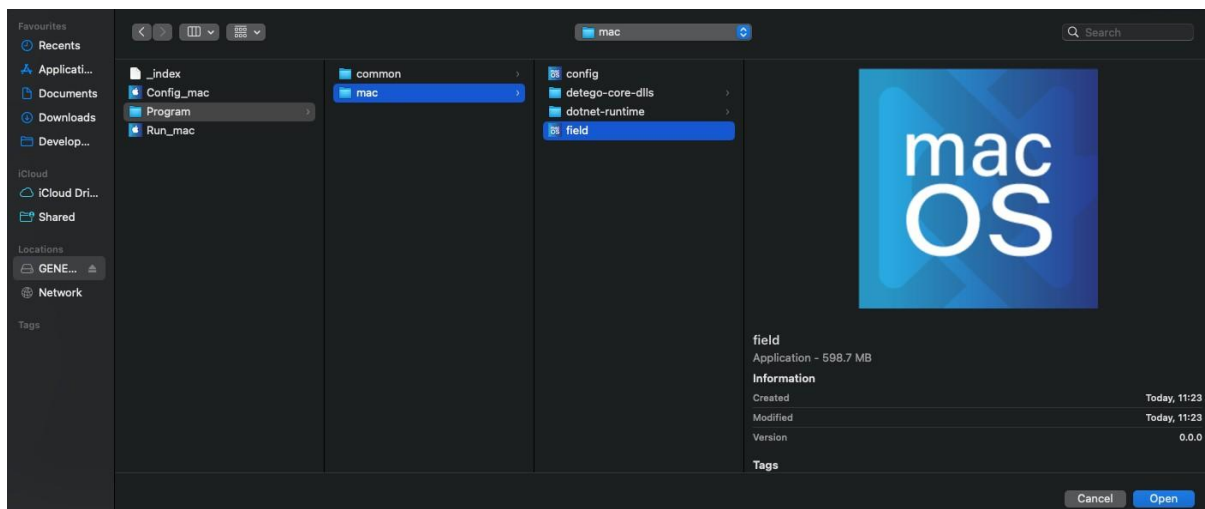


Figure 5

5. Restart the App

- Quit X (if it's open).
- Reopen it from your USB drive.

Field should now have the necessary access to run properly.