

DETEGO

2026
R2 

USER MANUAL

LEGAL NOTICES

Copyright © 2026 Mobile Content Management Solutions. All rights reserved.

Detego Global is the registered trading name of Mobile Content Management Solutions (MCM Solutions, MCMS) Limited.

This user manual is delivered subject to the following conditions and restrictions:

This manual contains confidential, proprietary information which belongs to Mobile Content Management Solutions Ltd. This information is supplied in the strictest confidence for the explicit and sole purpose of assisting authorised users of Detego in using the software.

No part of this content may be used for any other purpose, disclosed to any person or firm, or reproduced by any means, electronic or mechanical, without the express prior written permission of MCM Solutions.

The text and graphics are for illustrations and reference only. The specification on which they are based is subject to change without notice.

Information in this document is subject to change without notice. Unless otherwise noted, corporate and individual names and data used in the examples herein are fictitious.

Detego Ballistic Imager is a globally patented technology.

Detego Field Triage is a globally patented technology.

For more information, please get in touch with us at +44 (0) 1403 267 176 or marketing@detegoglobal.com.

TABLE OF CONTENTS

1.	INTRODUCTION	5
1.1.	SYSTEM REQUIREMENTS	6
1.2.	DETEGO MODULES	7
1.3.	MIGRATING CASES FROM LEGACY VERSIONS.....	8
2.	DETEGO ANALYSE OVERVIEW	10
2.1.	THE DETEGO ANALYSE HOME SCREEN.....	10
2.2.	NAVIGATION PATH	10
2.3.	INFORMATION	11
2.4.	USER DROPDOWN.....	12
2.5.	HELP.....	13
2.6.	CONFIGURATION.....	15
3.	DETEGO ANALYSE CONFIGURATION.....	16
3.1.	CONFIGURING SYSTEM SETTINGS.....	17
3.2.	CONFIGURING TAGS	30
3.3.	CONFIGURING JOB QUEUES	36
3.4.	CONFIGURING HASHLISTS	43
3.5.	CONFIGURING FACE WATCHLISTS	57
3.6.	CONFIGURING YARA RULES	63
3.7.	CONFIGURING FIELD PROFILES	68
3.8.	CONFIGURING KEYWORD/REGEX LISTS.....	73
3.9.	CONFIGURING STORAGE VOLUMES.....	79
3.10.	CONFIGURING NON-EVIDENCE VOLUMES.....	82
3.11.	CONFIGURING REMOTE ACQUISITION SETTINGS	84
3.12.	CONFIGURING EXTRACTION OPTIONS	85
4.	ACQUIRE CONNECTED MEDIA	87
4.1.	AUTO-DETECT	88
4.2.	WRITE BLOCKING	89
4.3.	DETEGO ANALYSE DISK INSPECTOR	90
4.4.	PHYSICAL DISK.....	93
4.5.	MOUNTED DRIVE.....	97
4.6.	IMAGE FILE	99
4.7.	DIRECTORY	101
4.8.	MOBILE AND TABLET	103
4.9.	NETWORK AGENT.....	116
5.	DETEGO FIELD DEVICES	117
5.1.	DETEGO FIELD CHANGE LIST - DISCLAIMER.....	117
5.2.	LICENSING FIELD DEVICES.....	119

5.3.	DETEGO FIELD LEGACY - WINDOWS 7 COMPATIBLE	122
5.4.	LICENSING BOOT DEVICES	123
5.5.	ADDING HASHLISTS AND KEYWORD / REGEX LISTS.....	125
5.6.	ADDING FIELD PROFILES	127
5.7.	CREATING ADDITIONAL BALLISTIC COLLECTORS.....	128
5.8.	RUNNING DETEGO FIELD ON WINDOWS AND MACOS	129
5.9.	DETEGO FIELD CONFIG.....	134
5.10.	DETEGO HASHLIST CONVERTER.....	204
5.11.	COVERT BOOKING PAGE	205
5.12.	DETEGO FIELD REPORTS.....	209
5.13.	IMPORTING DETEGO FIELD/BALLISTIC	211
5.14.	CLEANING AND REVOKING FIELD DEVICES	216
6.	ANALYSE AND MANAGE.....	219
6.1.	CASE MANAGEMENT	220
6.2.	IMPORTING EXHIBITS.....	256
6.3.	EXPORTING EXHIBITS.....	269
6.4.	THE CASE MANAGEMENT HOME SCREEN	279
6.5.	DETEGO OMNIVIEWER.....	289
6.6.	TIMELINE VIEW.....	299
6.7.	FILE FILTERING	313
6.8.	FILE SORTING	322
6.9.	THE PORTABLE VIEWER	329
6.10.	ANALYTICS.....	342
6.11.	DATA PREPARATION ANALYTICS	343
6.12.	DATA CLASSIFICATION ANALYTICS.....	363
6.13.	DATA EXTRACTION ANALYTICS	378
6.14.	MEDIA PROCESSING ANALYTICS	399
6.15.	PASSWORD PROCESSING ANALYTICS	411
6.16.	REPORTS	415
6.17.	AUDIT LOG	425
6.18.	FUSION	427
7.	TROUBLESHOOTING	440
8.	BIOS KEYS	442

1. INTRODUCTION

The Detego® Unified Forensics Platform is an end-to-end investigation suite to acquire, analyse, and report on data from digital devices. The latest generation of the platform, 2026 R2, gives the investigator the power to acquire data from smartphones, tablets, laptops, PCs, and external drives and allows extensive data analysis.

The amalgamation of this big data into one central command centre allows you to extract maximum intelligence from it and find the critical links to your case using automated workflow technology. As intuitive as it is functional, the Detego® Unified Forensics Platform is used by the world's elite military units, intelligence agencies, law enforcement agencies and major enterprises within both field and lab-based environments.

Figure 1



PLEASE NOTE! We strongly advise that any forensic tools run using an administrator user and administrator mode to prevent the loss of crucial functionality. They need access to parts of the OS that are unavailable to standard users.

CAUTION! The latest version of this User manual can be found on our secure customer portal, containing any revisions that might not be included in the Detego in-built version.

1.1. SYSTEM REQUIREMENTS

Detego Analyse can run on most high-end Windows 10/11 devices (PC, laptop or tablet); however, using a high-powered device will allow you to run analytical processes and tasks significantly faster.

Figure 2

	MINIMUM/BASIC SPECIFICATION ¹	RECOMMENDED SPECIFICATION
Processor (CPU)	Intel i5 Quad Core (2017 or newer) - Geekbench single core speed of 1200 or greater.	Intel i7 Octa-Core (2022 or newer) - Geekbench single-core speed of 2200 or greater.
Memory (RAM)	8GB ²	32GB +
Storage	SSD with 200GB free for installation. *Additional space required for data collections.	2TB SSD +
Ports	2x USB 3.0	1x Thunderbolt 3 3x USB-C / USB 3.1 1x USB 3.0
Graphics Card (GPU)	No GPU required for basic usage. Minimum of 4GB NVIDIA 2016 Pascal generation or newer with latest drivers installed.	8GB+ NVIDIA, 2022 Ada Lovelace generation or newer with latest drivers installed.
Operating System (OS)	Win 10/11 Pro 64-bit	Win10/11 Pro 64-bit
Windows Build	1607 and above	1607 and above

Please note that running Detego Analyse on a Hard Disk Drive (HDD-spinning Platter Drive) is NOT supported⁵ due to its severe performance limitations and can sometimes lead to unresponsiveness and timeouts. We recommend using a Solid-State Drive (SSD) for your main Operating System drive to eliminate this issue.

- **RAID support for storage volumes is limited.**
- **Detego Analyse is currently NOT supported to run on a Windows Virtual Machine.**
- **A write-blocking device will ensure forensically sound images, provide high assurances that data will not be modified during the acquisition process, and ultimately ensure data integrity.**
- **The minimum screen resolution required is 1366 x 788. Please adjust Windows display settings and Detego UI Scaling for complete application visibility.**

¹ Whilst Detego Analyse is supported to function on these minimum specifications, its performance and capabilities may be highly compromised.

² The Detego installer requires at least 6144MB of usable RAM. Detego Analyse functionality requires 16GB of RAM minimum.

³ Detego installation can fit on this size drive; however, you may require more storage space or external drives for your exhibits.

⁴ Some analytical processes, such as Video Frame Processor, use dedicated GPU performance to run effectively. Running such processes on larger exhibits without a GPU could cause system unresponsiveness and prolonged processing times.

⁵ HDDs are still supported as mass storage volumes due to their large capacity; however, we do not recommend them as there will be significant time overhead on processing.

1.2. DETEGO MODULES

The Detego® Unified Forensics Platform comprises a series of modules that can be used standalone or combined for optimum effect. You may have purchased only specific modules.

The modules are:

DETEGO ANALYSE AI+ WITH FUSION

The central hub for all data collected by the Detego acquisition modules. It has hundreds of analytical processes to help accelerate your investigation and configuration options to pre-configure bespoke workflows.

Detego Fusion allows you to conduct advanced link analysis across your digital exhibits, including PCs, laptops, mobile phones, smartphones, tablets, USB devices and other removable media (SD cards, portable external drives, IDE and SATA drives, etc.).

DETEGO MEDIA ACQUISITION

A forensic acquisition tool for acquiring and viewing data from USB devices and other removable media (SD cards, micro SD cards, portable external drives, IDE & SATA drives, etc.).

DETEGO FIELD TRIAGE

A fully portable digital forensic solution for field-based investigators to acquire and act on data from PCs, laptops and servers. Includes intuitive warning technology that automatically alerts the user of any suspicious items on the target device through a red, amber, or green status alert.

DETEGO BALLISTIC IMAGER

The world's fastest patented forensic imaging tool for PCs, laptops and servers, capable of copying a disk drive in minutes.

DETEGO MD POWERED BY GMDSOFT

Built on the industry-leading GMDSOFT MD-Series, this is the complete solution for data extraction from a comprehensive range of more than 15,000 mobile device models. It supports physical and logical extraction methods for Android, Apple iOS, Windows, Tizen OS and other mobile operating systems.

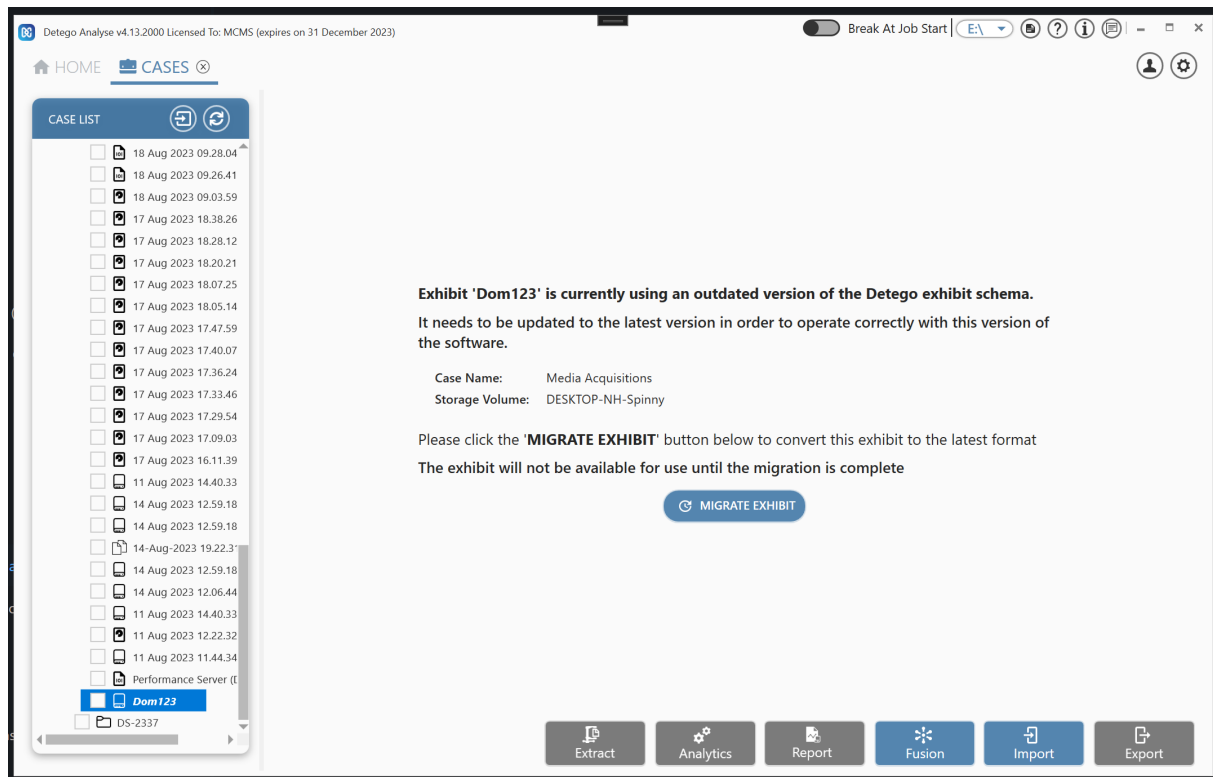
DETEGO FOR MOBILE DEVICES

A purpose-built software solution designed to create an iOS or Android device backup. This is for very basic backups only.

1.3. MIGRATING CASES FROM LEGACY VERSIONS

Detego Analyse supports converting legacy (pre-v4.12) exhibits into the new database format. When an exhibit needs to be converted, it will appear italicised in the case list, and the following screen will appear when it is selected:

Figure 3



Clicking the MIGRATE EXHIBIT will initiate a conversion job. Conversion can be cancelled if necessary; however, the exhibit will not be usable in Detego 2025.2 until migration is completed.

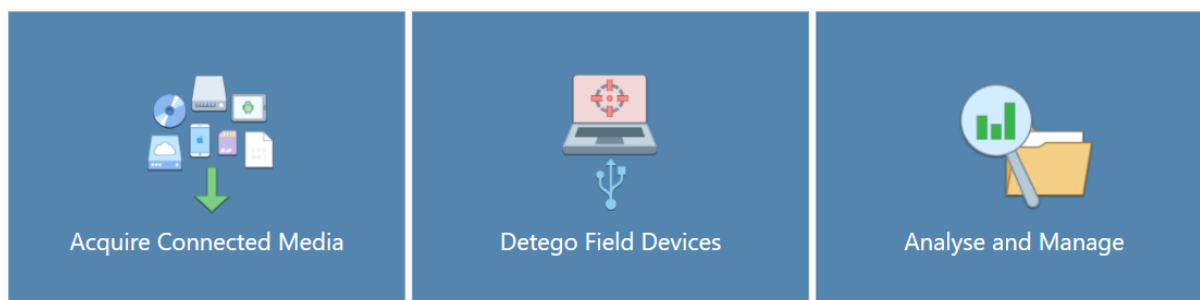
WARNING! Before upgrading, please import and revoke all licensed Detego Field and Ballistic devices to prevent data loss and any Field device issues.

2. DETEGO ANALYSE OVERVIEW

2.1. THE DETEGO ANALYSE HOME SCREEN

Detego Analyse is the command centre for all your cases and exhibits, complete with detailed analytical processes to help you investigate your case further and identify pertinent intelligence.

Figure 4



Once Detego Analyse has opened, the home screen displays three tiles:

- ***Acquire Connected Media***
- ***Detego Field Devices***
- ***Analyse and Manage***

Hovering your cursor over a tile will display a short overview of the tool's functionality at the bottom of the window.

2.2. NAVIGATION PATH

While using Detego Analyse, the user's navigation path is shown at the top of the screen, with the active workspace highlighted and underlined.

- Click on the screen name to quickly navigate to any previously accessed screens in the current session.
- Select the (x) on an open tab to close that tab.

Figure 5



2.3. INFORMATION

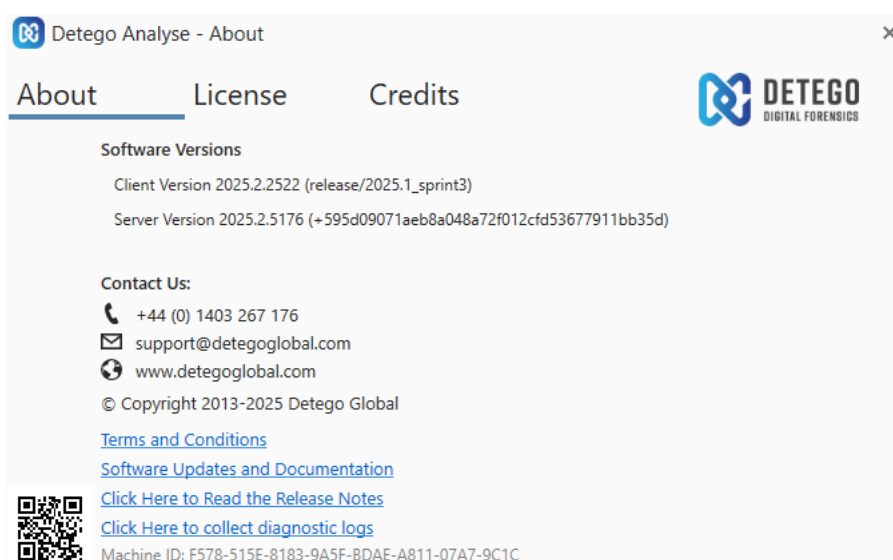
The (i) icon in the top right corner of the screen gives the user access to three [3] tabs:

ABOUT

This tab contains basic information about Detego and various links to access helpful content. It includes:

- Detego Client and Server Software Versions
- Contact Information
- Copyright Information
- Link to Terms and Conditions
- Link to Software Updates and Documentation
- Release Notes
- Access to collect Diagnostic Logs.
- Machine ID

Figure 6



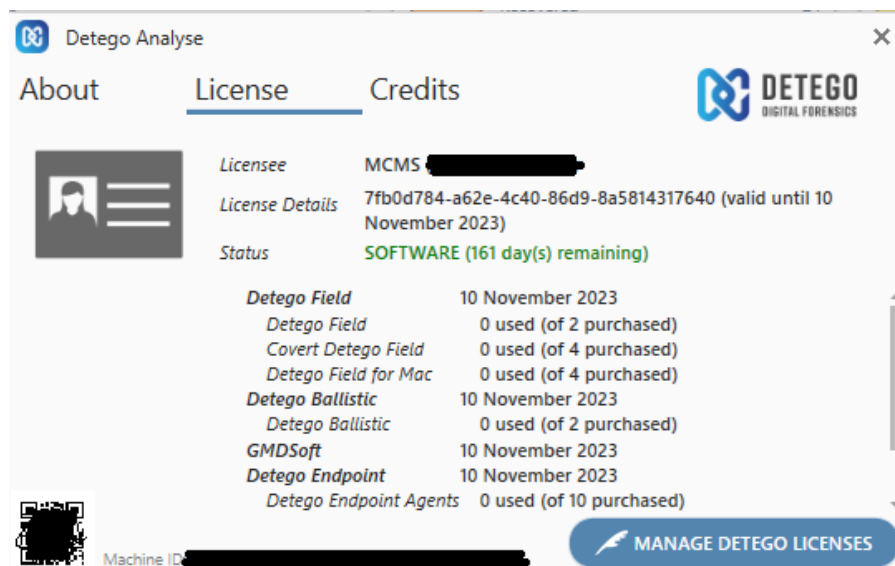
LICENSE

This tab shows your licensing information, including:

- License Name - (Usually your Company/Organisation name with your name in brackets).
- License Details - Your Unique license string or serial number depends on whether you have a license dongle or a software license.
- Status - The Status of your license.

Access to manage your license, including requesting a Trial, Purchase, Renewing or Applying a license.

Figure 7



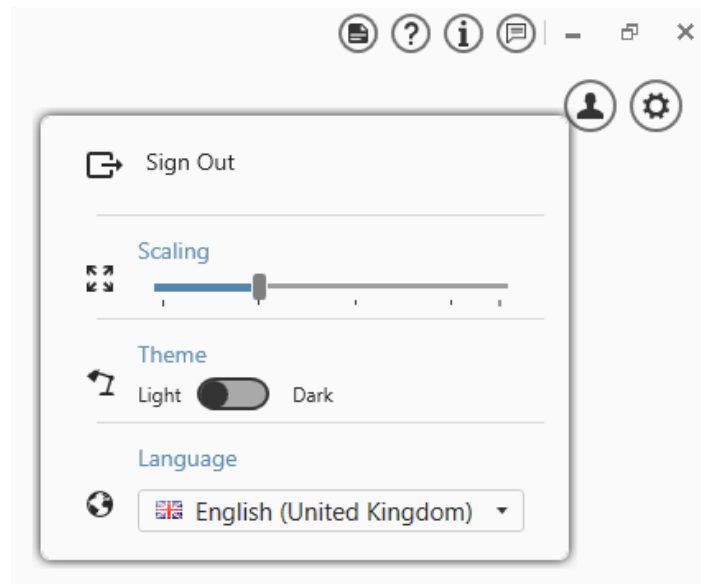
CREDITS

This tab displays the licensing for imagery used within the software.

2.4. USER DROPDOWN

The dropdown at the top right of the screen displays the user who is logged into Detego Analyse. By selecting the dropdown option, the user is presented with the options below:

Figure 8



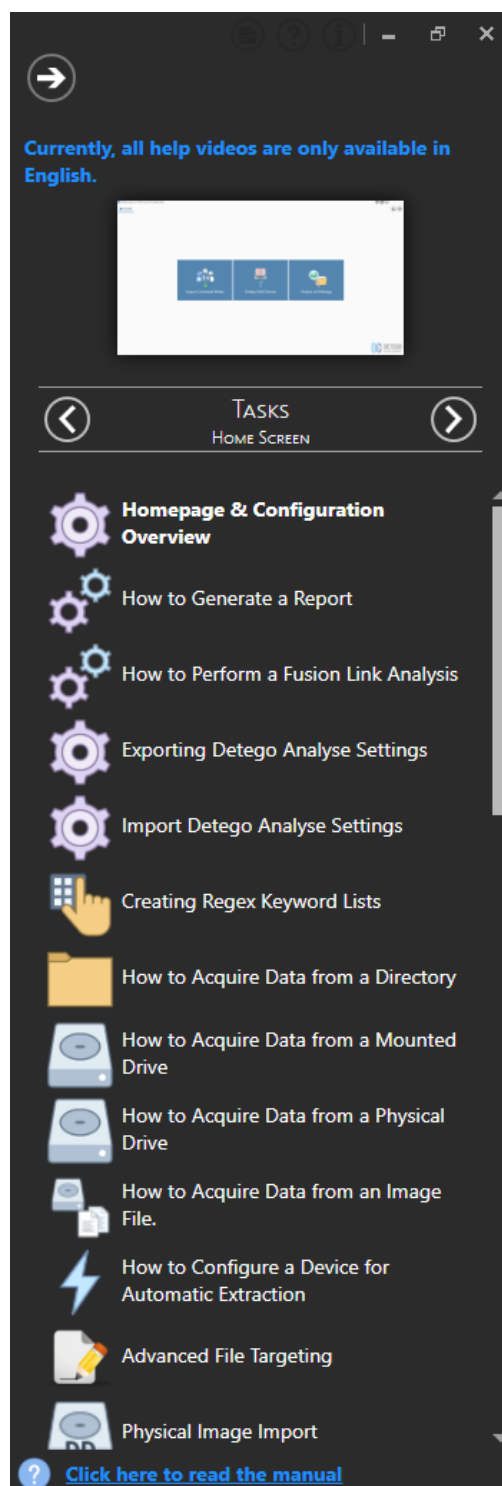
From here, the user can:

- Sign out of Detego (This will close Detego and reopen it automatically, keeping any jobs running in the background).
- Change the scaling of the window. We recommend using the default setting for the best appearance.
- Switch the toggle between Light mode (Default) and Dark mode.
- Select the language you wish to use; the default is English.

2.5. HELP

The Help question mark icon (?) opens the Help section.

Figure 9



You can view the available help videos for each topic; the videos displayed change based on the location of the application. You can also select the button at the bottom to open the inbuilt User guide.

2.6. CONFIGURATION

The Configuration Cog icon gives users access to the configuration settings, including System, Tags, Job Queues, Hashlists, Face Watchlists, Detego Field Profiles, Keyword Lists, Storage and Non-Evidence drives, Remote Acquisition and Extraction Options. For more information, see the next section.

3. DETEGO ANALYSE CONFIGURATION

Detego Analyse Configuration allows the user to configure the settings of Detego Analyse as well as manage their Job Queues, Hashlists, Keyword Lists, etc.

Select the 'Configuration' cog in the top right corner.

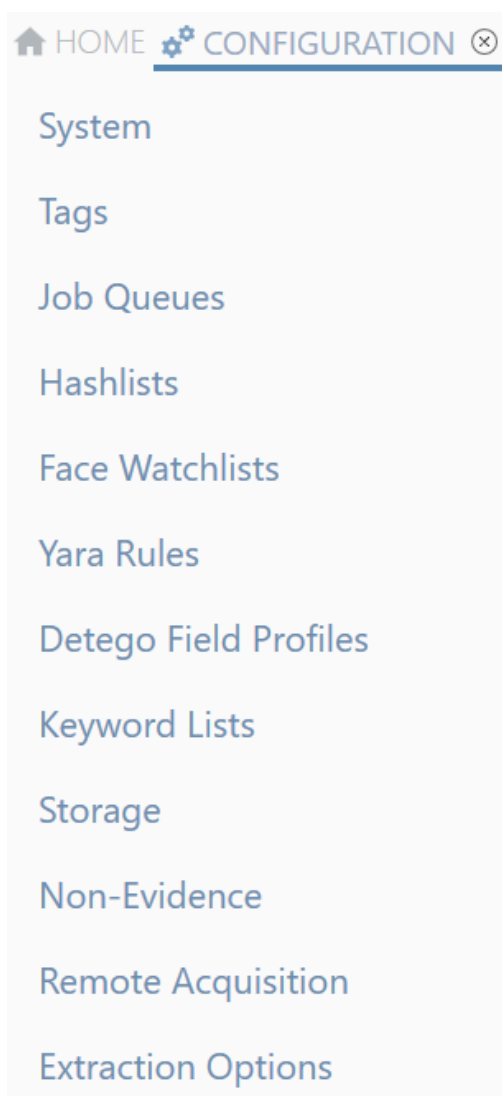
Figure 10



The below options to configure are listed below:

- System
- Tags
- Job Queues
- Hashlists
- Face Watchlists
- Yara Rules
- Detego Field Profiles
- Keyword Lists
- Storage
- Non-Evidence
- Remote Acquisition
- Extraction Options

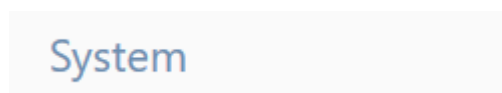
Figure 11



3.1. CONFIGURING SYSTEM SETTINGS

This section allows you to configure the basic System settings for Detego Analyse.

Figure 12



The following are available to configure within the System Settings:

- Dialog Box Settings
- Android Debug Bridge

- Mapping Provider
- Camera Setup
- GPU/CPU Device Setup
- Image Options
- Screen Recording Setup
- Detego Field Settings
- Project VIC Hash List Import Settings
- Report Configuration
- File System Paths
- Export/Import System Settings

NOTE! To save your changes, ensure you select the 'Save' icon at the top right corner of the System Settings screen. Alternatively, select the 'Discard' icon to discard any changes made to the System Settings.

Figure 13



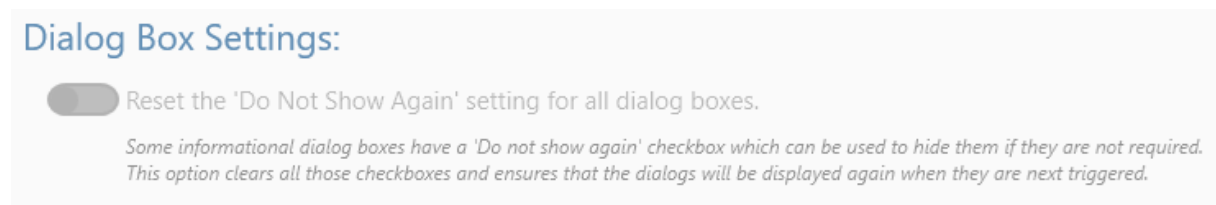
DIALOG BOX SETTINGS

The toggle within the Dialog Box Settings section allows you to reset the 'Do Not Show Again' setting for all dialog boxes.

Any informational dialog boxes on which you selected the 'Do Not Show Again' checkbox will be reset so they can trigger again.

This option will be greyed out if no 'Do Not Show Again' checkbox has been selected within any dialog boxes or if they have already been reset.

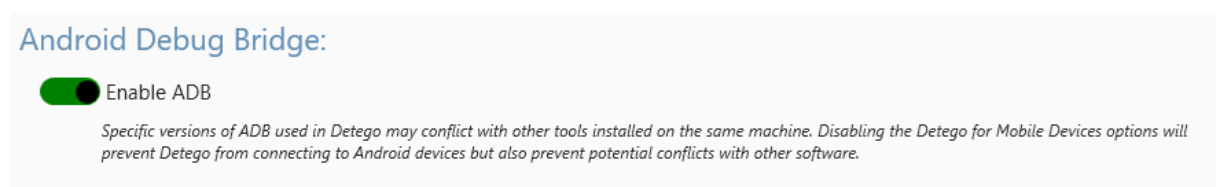
Figure 14



ANDROID DEBUG BRIDGE

ADB (Android Debug Bridge) lets you connect Android mobile devices to Detego, enabling mobile device extractions. Please note that you will need access to Detego MD powered by GMDSOFT to perform extractions via Detego. Turning off this toggle will disallow mobile extractions via Detego; the feature is enabled by default.

Figure 15



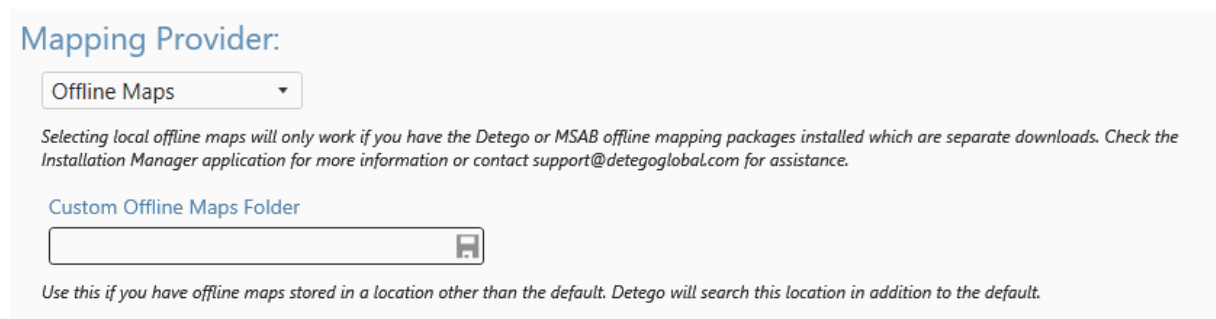
MAPPING PROVIDER

The Mapping Provider dropdown allows you to select your preferred map provider within Detego. Changes to this won't be activated until the SAVE button has been selected.

These include:

- Open Street Map (Default)
- Google Maps
- Offline Maps

Figure 16



The screenshot shows a window titled 'Mapping Provider:'. At the top, there is a dropdown menu with 'Offline Maps' selected. Below this, a note states: 'Selecting local offline maps will only work if you have the Detego or MSAB offline mapping packages installed which are separate downloads. Check the Installation Manager application for more information or contact support@detegoglobal.com for assistance.' Underneath the note is a section labeled 'Custom Offline Maps Folder' with a text input field and a folder icon button. A final note at the bottom says: 'Use this if you have offline maps stored in a location other than the default. Detego will search this location in addition to the default.'

When selecting the 'Offline Maps' mapping provider, a new option will appear for specifying an additional folder where Detego Analyse will look for offline mapping files. From v4.18 and up, the mapping supports both the existing (now legacy) .mbtiles mapping files and the newer (.ctm1) mapping files.

In offline mapping mode, the following directories will be searched:

- C:\ProgramData\Detego\OfflineMaps
- C:\ProgramData\MSAB\Maps\OfflineMaps
- The folder specified by the 'Custom Offline Maps Folder' system setting.

Detego Analyse will currently prioritise offline mapping files found using the legacy .mbtiles format. Only if no .mbtiles files are found will the newer .ctm1 files be used.

The legacy .mbtiles offline mapping supports only a single (first) mapping file found. If using the .ctm1 format then multiple mapping files will be merged in the mapping view within Detego Analyse. This is useful if combining multiple smaller regions without having to include the entire world.

If you wish to use the Legacy .mbtiles Offline Mapping package please note that it is approximately 70GB and can be downloaded from the Detego Install Manager from the 'CUSTOM' options. As a result, it can take a considerable time to download on slower internet connections.

If you wish to use the .ctm1 files but have the legacy .mbtiles then you will need to make sure you remove these from the following folder:

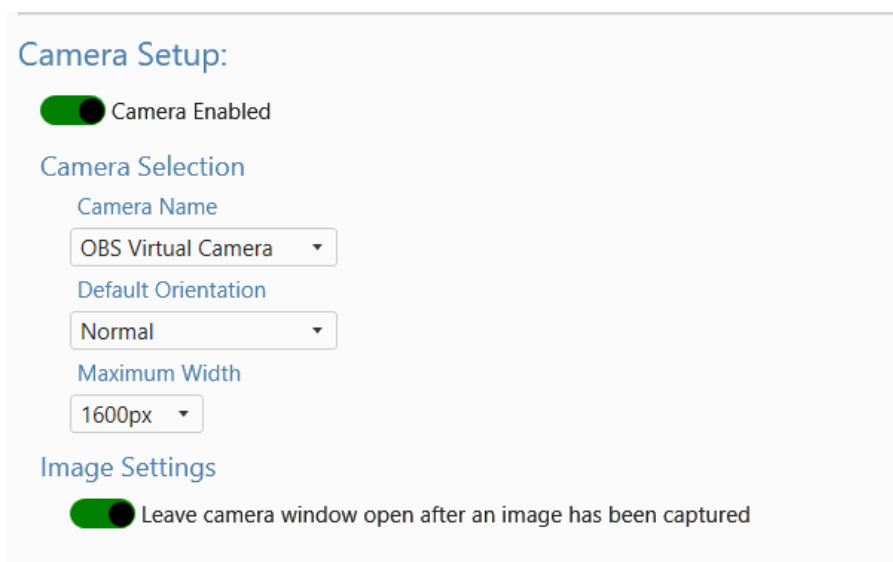
- C:\ProgramData\Detego\OfflineMaps

CAMERA SETUP

The Camera tool allows users to take images relating to an exhibit or case. This feature requires a camera or connected screen recorder.

- Camera Enabled - This toggle button enables the use of the camera within Detego.
- Camera Name - This dropdown will display the available cameras connected to the machine.
- Default Orientation - This dropdown allows you to select the default orientation between:
 - Normal
 - Inverted
- Maximum Width - This dropdown will list the maximum width in pixels.
- Image Settings - This toggle button allows you to select whether the camera window will stay open after capturing an image.

Figure 17



The screenshot shows the 'Camera Setup' window. It has a title bar and a light gray background. The settings are organized into sections: 'Camera Enabled' with a green toggle switch; 'Camera Selection' with a 'Camera Name' dropdown set to 'OBS Virtual Camera'; 'Default Orientation' with a dropdown set to 'Normal'; 'Maximum Width' with a dropdown set to '1600px'; and 'Image Settings' with a green toggle switch labeled 'Leave camera window open after an image has been captured'.

GPU/CPU DEVICE SETUP

The **GPU/CPU Device Setup** feature in *Detego Analyse* allows users to configure their preferred processing device for executing AI jobs. This functionality is part of the **Configuration Settings** and is designed to optimize the performance of AI tasks by leveraging available hardware resources.

KEY FEATURES:

- **Automatic Detection:** On server startup, the system automatically detects available GPU devices on the user's machine and saves this information, ensuring that the GPU options are up-to-date and ready for use.
- **User Selection:** Users can access the GPU/CPU Device Setup by navigating to the Configuration Settings in Detego Analyse and scrolling to the respective section. Here, users can view all available devices on their machine, including CPU, Intel GPUs, and other GPU devices such as NVIDIA GPUs.
- **Device Options:** The setup interface displays the detected devices, allowing users to choose their desired processing unit for AI jobs. Selecting a GPU enables GPU acceleration while choosing a CPU executes AI tasks using the CPU.

GPU/CPU SETTING OVERVIEW

The figure below shows the **GPU/CPU Device Setup** section, which has a drop-down menu listing all available processing devices. Users can select any option, such as Auto Detect, NVIDIA GPU, or CPU.

Once a device is selected, the system displays detailed information about it, including the **device type, driver date, driver version, and status**, ensuring that users have all the necessary information about the selected processing unit.

Figure 18



USAGE INSTRUCTIONS:

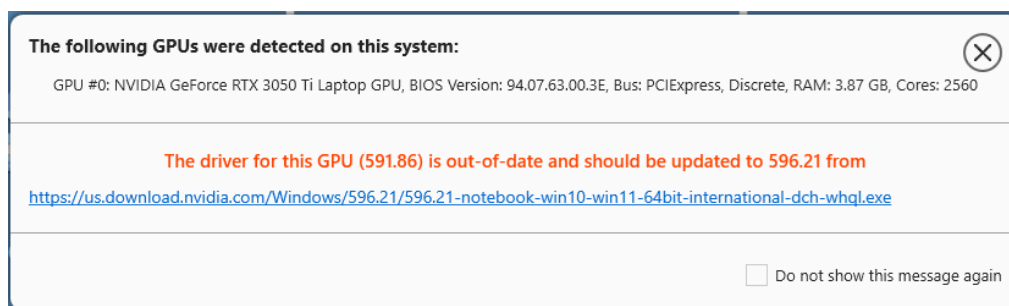
- **Accessing the Setup:** Navigate to the Configuration Settings in Detego Analyse and scroll to the GPU/CPU Device Setup section.
- **Selecting a Device:** From the drop-down menu, select the preferred processing device for running AI jobs.
- **Confirmation:** The system will display the details of the selected device, confirming the configuration.

This feature ensures that users can optimize AI job performance by selecting the most suitable processing unit available on their machine. It provides flexibility and enhances the efficiency of AI tasks within Detego Analyse.

GPU DRIVERS:

Sometimes your GPU drivers become outdated. When this occurs, Detego Analyse displays a dialog box with details advising you to install the latest drivers. This may appear as shown below:

Figure 19

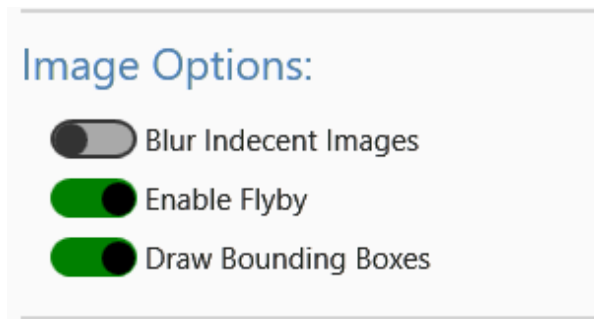


Outdated drivers can cause performance and functionality issues in GPU-utilised jobs so please ensure you update them regularly.

IMAGE OPTIONS

Image Options allow you to blur indecent images, redact information and protect your team.

Figure 20



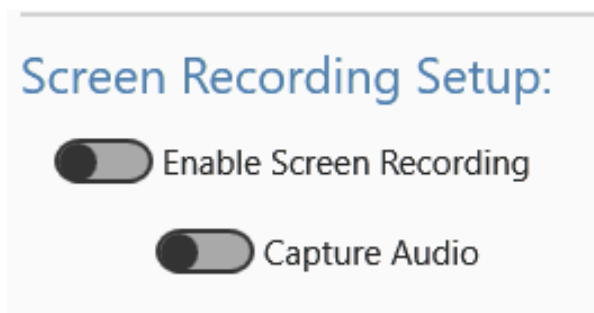
- **Blur Indecent Images** - Enabling this will blur any indecent images within your exhibit. (Disabled by default).
- **Enable Flyby** - Disabling this will switch off the flyby functionality to prevent indecent images from being displayed within the exhibit jobs. (Enabled by default).
- **Draw Bounding Boxes** - Disabling this will not allow you to draw bounding boxes, which restricts the viewing of files. (Enabled by default).

SCREEN RECORDING SETUP

The Screen Recording feature allows you to record evidence items that generate a video report.

- **Enable Screen Recording** - This toggles the Screen Recording tool on or off. (Off by default).
- **Capture Audio** - This toggles on or off the capture of audio with Screen Recording (it is off by default).

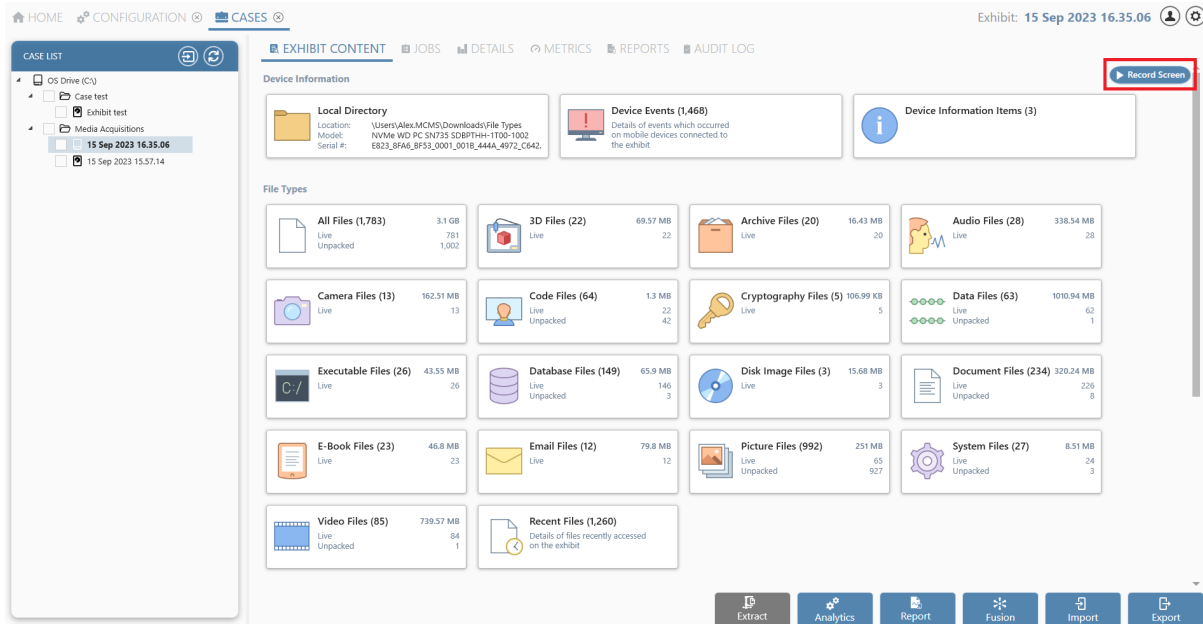
Figure 21



Follow these steps to configure the screen recording feature:

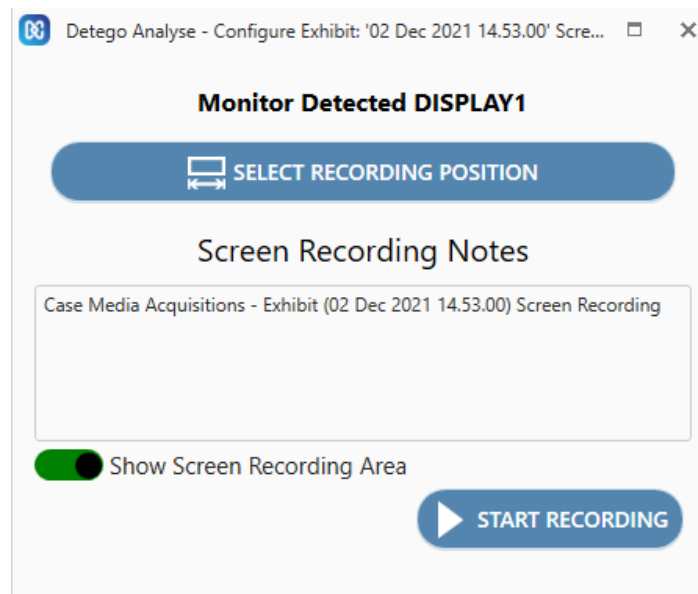
- Once you have enabled the Screen Recording toggle, a button will be displayed in the 'Exhibit Content' section in the top right corner.

Figure 22



- Selecting RECORD SCREEN will display a pop-up with configuration options.

Figure 23



- Clicking the 'SELECT RECORDING POSITION' allows you to change the area of the screen you wish to record.

Figure 24

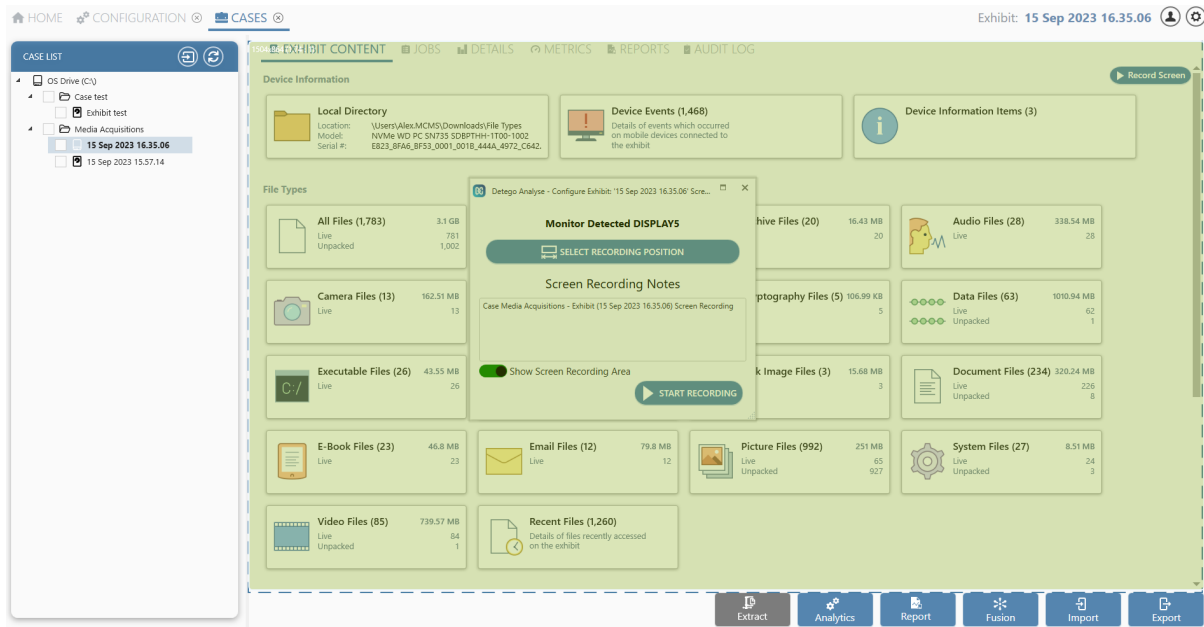
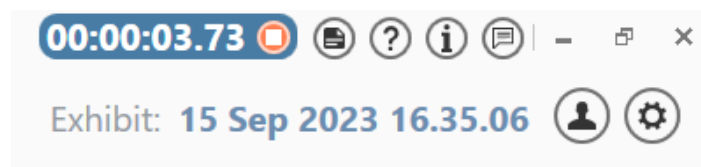
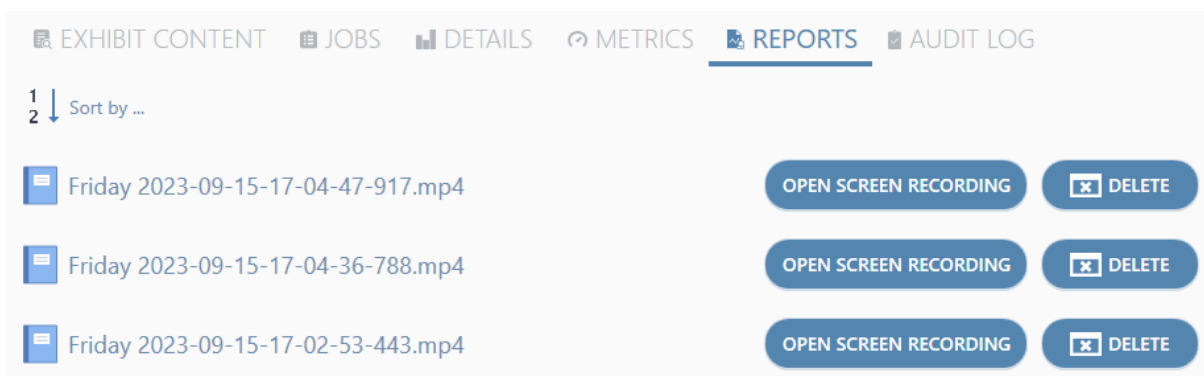


Figure 25



- Once stopped, the recording can be found in the 'Reports' tab of the case, where you can open the screen recording or delete it.

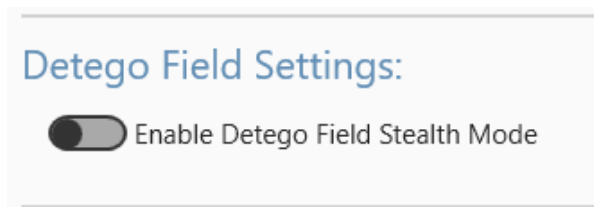
Figure 26



DETEGO FIELD SETTINGS

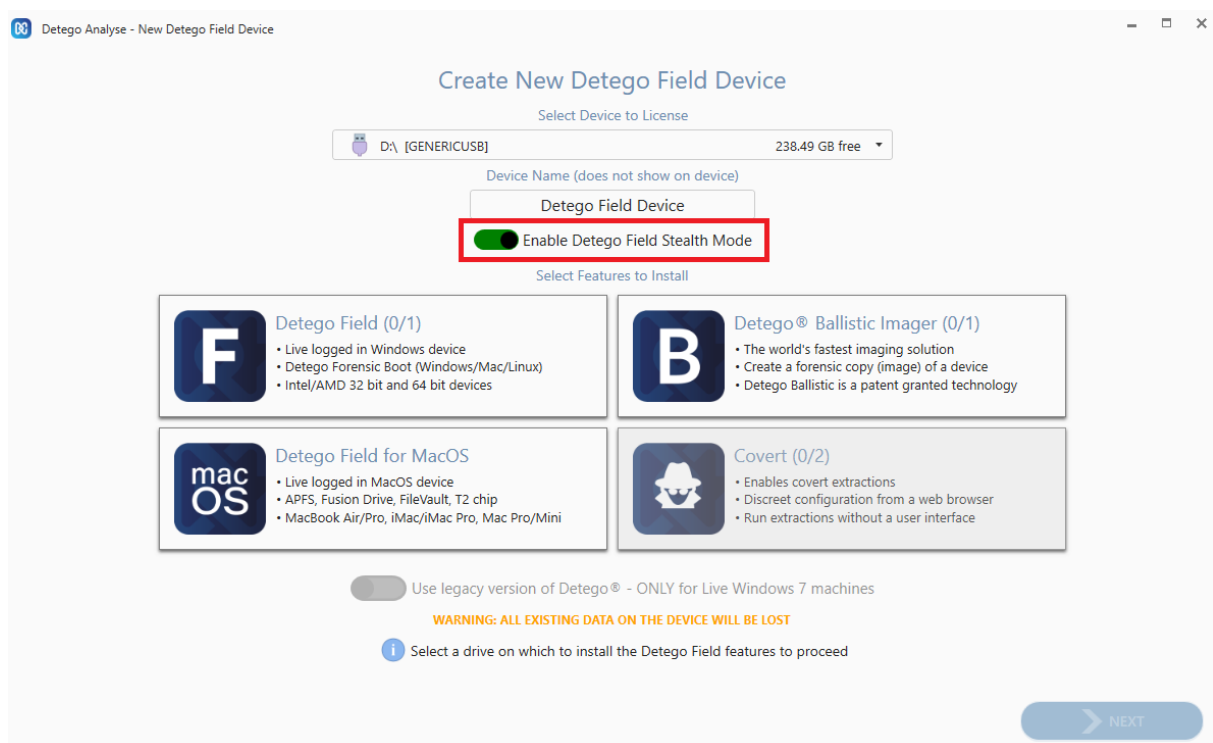
The Detego Field Setting allows users to toggle stealth mode on by default for all Detego Field devices created from that instance of Detego Analyse (it is off by default).

Figure 27



This can be overridden when creating a Detego Field Device by simply deselecting the toggle within the Detego Field Device Creation window.

Figure 28



PROJECT VIC HASH LIST IMPORT SETTINGS

The 'Include Ignorable' toggle allows you to change whether Project VIC hashes with an ignorable tag will be imported or not.

- ON - Project VIC hashes with an ignorable tag will be imported
- OFF - Project VIC hashes with an ignorable tag will be skipped

Figure 29

Project Vic Hash List Import Settings:

☒ Include Ignorable

REPORT CONFIGURATION

This section allows you to customise the reports you create in Detego.

Figure 30

Report Configuration:

☐ Display Logo and Name

Display Name :

No file chosen

☐ Include Post Analysis Information

- Display Logo and Name - This toggle button enables the logo and name to be displayed on reports.
 - Display Name - This text box allows you to type a name for your reports.
 - UPLOAD - This button allows you to select a logo suitable for your reports.
- Include Post Analysis Information - This toggle button lets you enable any post-analysis information you wish to include in your reports.
 - The text box below the toggle button includes the space to type the information you wish to have.

FILE SYSTEM PATHS

The 'File System Paths' option allows you to place various folders in specific locations of your choosing, allowing you to select locations of drives with more storage space.

Select the icon on the right to browse to the location you choose.

Figure 31

File System Paths:

PLEASE NOTE: These paths must reside on local (non-removable) drives

Temporary Data:	C:\ProgramData\detego\Temp	
Hashlist Databases:	C:\ProgramData\detego\Hashlists	
Facelists Folder:	C:\ProgramData\detego\Facelists	
Detego Field Profiles Folder:	C:\ProgramData\detego\Field Profiles	

CAUTION! When changing the Temporary Data path, please make sure it does not target the root folder of a drive. If selecting another drive, please create a folder within that drive and select it first.

EXPORT/IMPORT SYSTEM SETTINGS

In this section, you can configure your 'Export System Settings' to export from one instance of Analyse to another. You can 'Import System Settings', which allows you to import system settings from another Detego Analyse system.

NOTE! Before importing, ensure you have at least double the storage space required; currently, the import job needs to be able to extract the entire settings archive into a temporary folder to import the items. The settings export job also creates a copy of the files to be exported in a temporary folder and then compresses it into the target files.

Figure 32

Export System Settings ☐ Export All ☐ Keyword Lists ☐ Hashlists ☐ Face Watchlists ☐ System Settings ☐ Detego Field Profiles ☐ Job Queues ☐ Tags ☐ Global Filters  EXPORT 0 ITEM(S)	Import System Settings ☐ Replace existing items  IMPORT DATA
---	---

To export your System Settings, you can select 'Export All', which will export all System Settings, OR you can choose the categories you wish to export. These include Keyword Lists, Hashlists, System Settings, Detego Field Profiles, Job Queues and Tags.

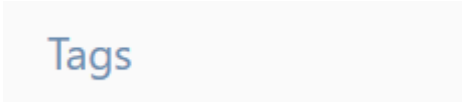
- Once you have selected appropriately, click the 'EXPORT # ITEMS' button and save the 'Detego Settings File' (.detego_settings) into a location.
- To import data into an instance of Detego, under the 'Import System Settings', select the 'IMPORT DATA' button and locate the appropriate 'Detego Settings File' (.detego_settings).

CAUTION! Ticking the 'Replace existing items' checkbox and then selecting the 'IMPORT DATA' button will overwrite your current settings, and you will lose your system settings. If you aren't sure you wish to do this, please export your System Settings before this to keep a copy.

3.2. CONFIGURING TAGS

Tags can mark files of interest, making identifying evidence, analysis and investigation quicker. They can also be assigned keyboard shortcuts for ease of use and an image stamp to help differentiate them.

Figure 33



Tags

CREATING NEW TAG GROUPS

To create a New Tag Group:

- From the Configuration window, select the 'Tags' tab on the left panel
- In the bottom right corner, select the 'NEW GROUP' button
- In the new pop-up window, name your Tag Group
- Select the icon you wish to use on the right side of the Name text box
- Select the toggle button to check whether the Tag Group is exclusive. You can only apply one tag within an exclusive group to a given taggable; any other tags within the same group applied to the taggable will be removed when applying a different one.

- Once you are happy with the details, select the SAVE button to save and create or CANCEL to cancel it.

Figure 34

CREATING A NEW TAG

To create a New Tag, follow the below steps:

- Click the 'NEW TAG' button in the bottom right corner of the screen.
- From the 'New Tag' pop-up window, follow the below sections.

Name and Group

- Input a Name for the Tag, and then choose a tag group from the dropdown to house the new Tag.

Image Stamp

- If you wish, you can select an image icon and a colour to identify the new tag.

Key Shortcut

- If you wish, you can create a keyboard shortcut by configuring the sliding buttons and dropdown fields.

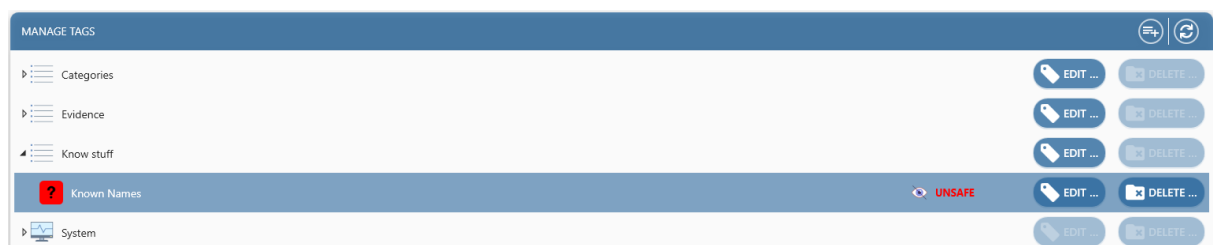
Viewable Status

- UNSAFE - If you wish, you can toggle this option to mark items with this Tag as Unsafe. Unsafe items will be marked as red and images and thumbnails will be blurred.
 - SAFE - If you wish, you can toggle this option to mark items with this Tag as Safe. Safe items will be marked as green and will be viewable.
 - REDACTED - If you wish, you can toggle this option to mark items with this Tag as redacted. Redacted items will be redacted from reports and exports.
- Click the 'SAVE' button to store the new tag.

Figure 35

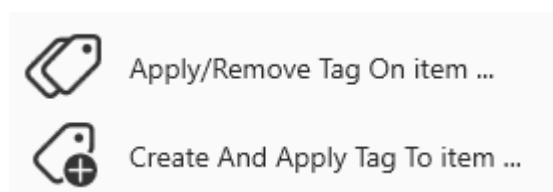
Once you have saved your Tag, you can view it from the MANAGE TAGS section. This screen allows you to EDIT or DELETE the Tags you have created.

Figure 36



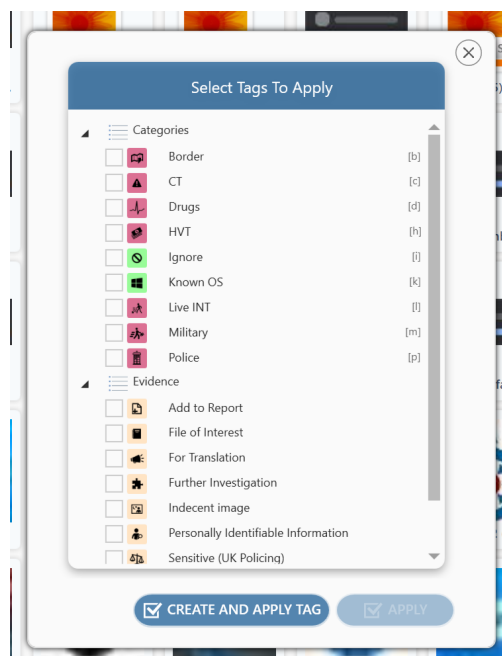
APPLY/REMOVE TAGS

Figure 37



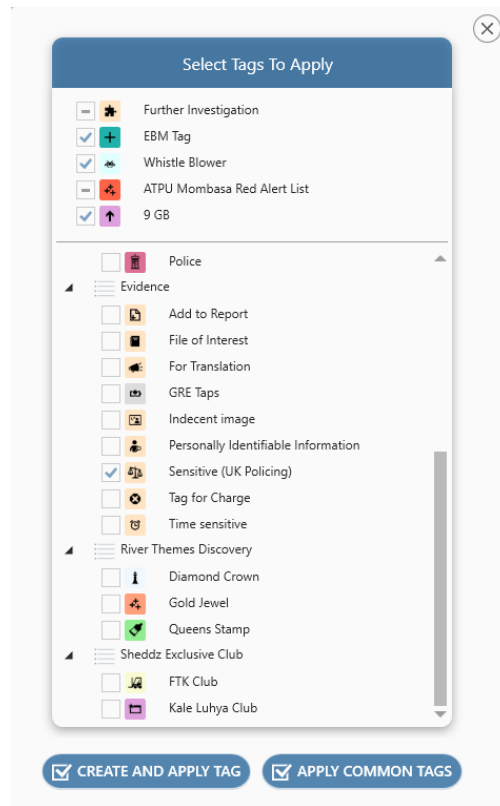
Clicking on the “*Apply/Remove Tag On Item*” menu item opens a pop-up window, enabling tag management in a more consolidated manner. Users can **Apply/Remove** tags to the selected items in the Evidence Browser by selecting the intended/desired tag checkboxes and clicking on the “**APPLY**” button, as shown in the figure below.

Figure 38



If more than one item is selected, tags commonly applied to the selected items are displayed at the top with their **checkboxes selected/checked**. In contrast, indeterminate checkboxes will be shown if tags are applied on some items but not all (see image below). The user can select any desired tags and click the “**APPLY COMMON TAGS**” button to apply/remove tags on the selected items.

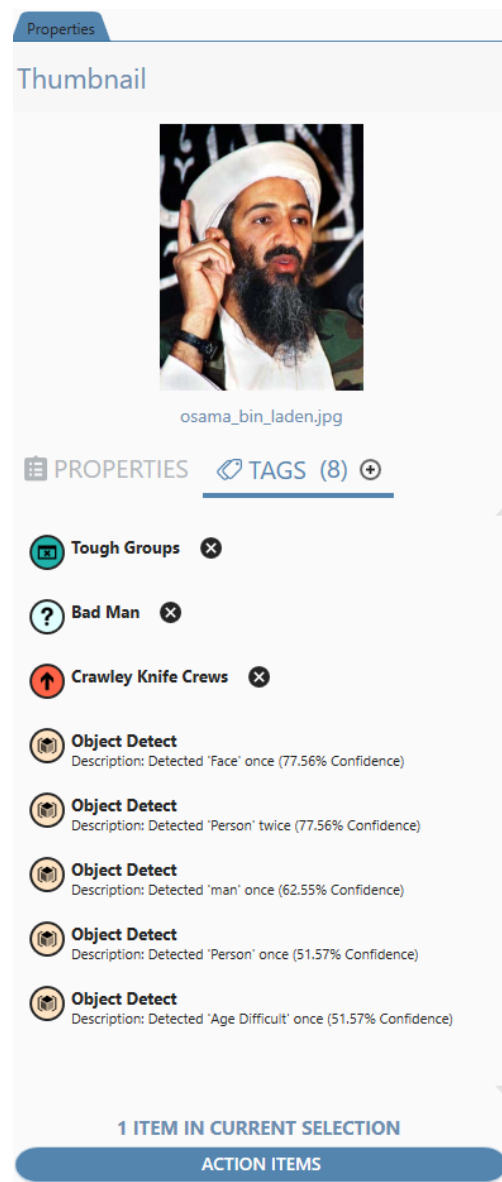
Figure 39



Upon Applying Tags, the Properties tab was modified as follows:

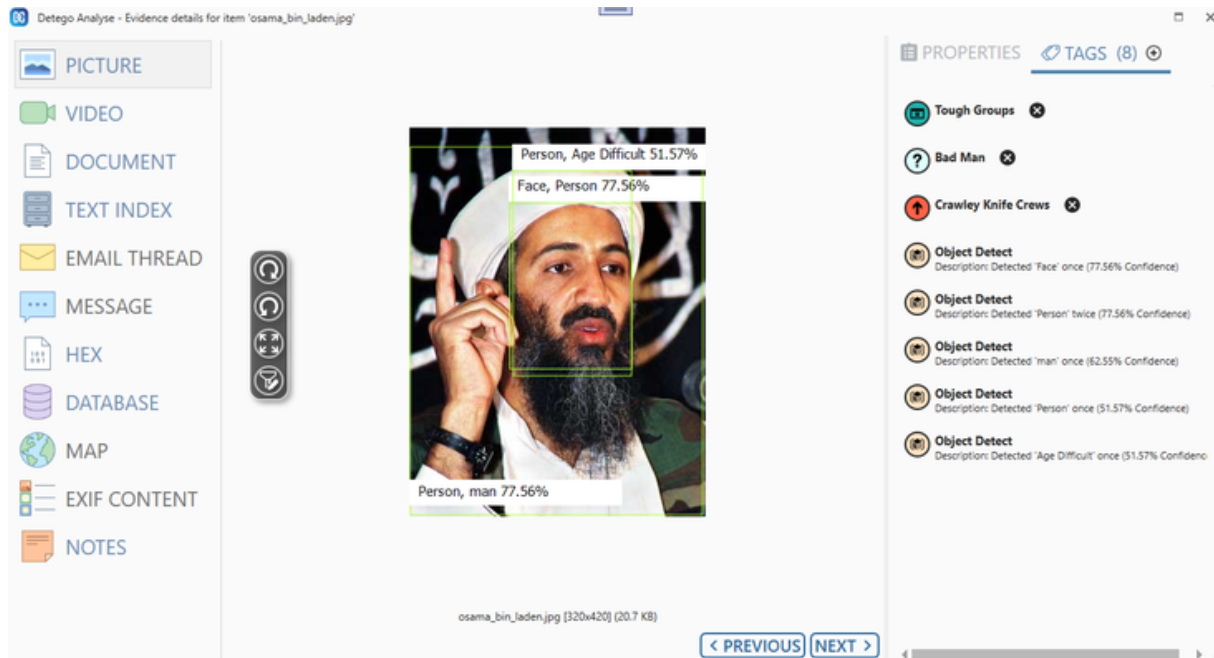
- The **Tags** and **Properties** tabs were added below the thumbnail, as shown in the figure below.
- The contents of the Properties Tab were maintained just as they appeared before.
- The Tags tab displays **tags applied** to the selected item in the Evidence browser. Each tag except for the "**System Tags**" has an "**x**" button to enable the removal of the tag from the selected item. If *multiple items are selected* in the browser, only "**Commonly Applied**" tags are displayed alongside the system tags. An "**Add Tags**" button in the Tags header opens the pop-up window to manage tags.

Figure 40



The Tags and Properties Tabs are also displayed in the **Omniviewer Window**, as shown in the figure below. Using the steps described above, the user can Apply or remove tags to the item displayed.

Figure 41



3.3. CONFIGURING JOB QUEUES

The Job Queue functionality allows you to define a series of jobs to run sequentially against an exhibit. Job Queues are designed to automate the manually intensive elements of the investigative process, from acquiring the data from an exhibit to running a series of analytical processes against it.

Job Queues can massively speed up the investigative process and reduce and even eliminate a backlog of cases.

Detego has some pre-configured job queues to assist with your workflow, but you can also create your own.

NOTE! Any job queue created before 2026.1 that includes acquisition jobs must be recreated to run correctly. Recreate job queues after upgrading to prevent any issues.

Figure 42

Job Queues

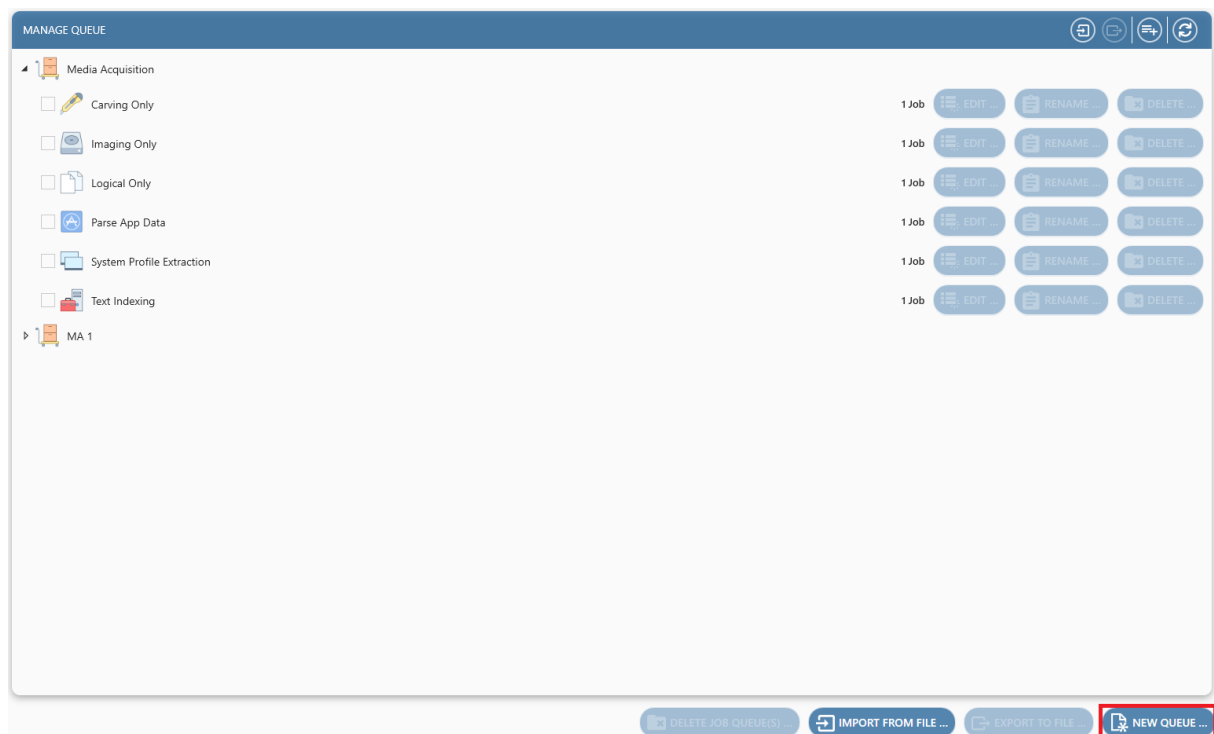
CREATING A NEW JOB QUEUE

Before creating your job queue, it is recommended that you familiarise yourself with the available jobs.

To create a job queue, follow the below steps:

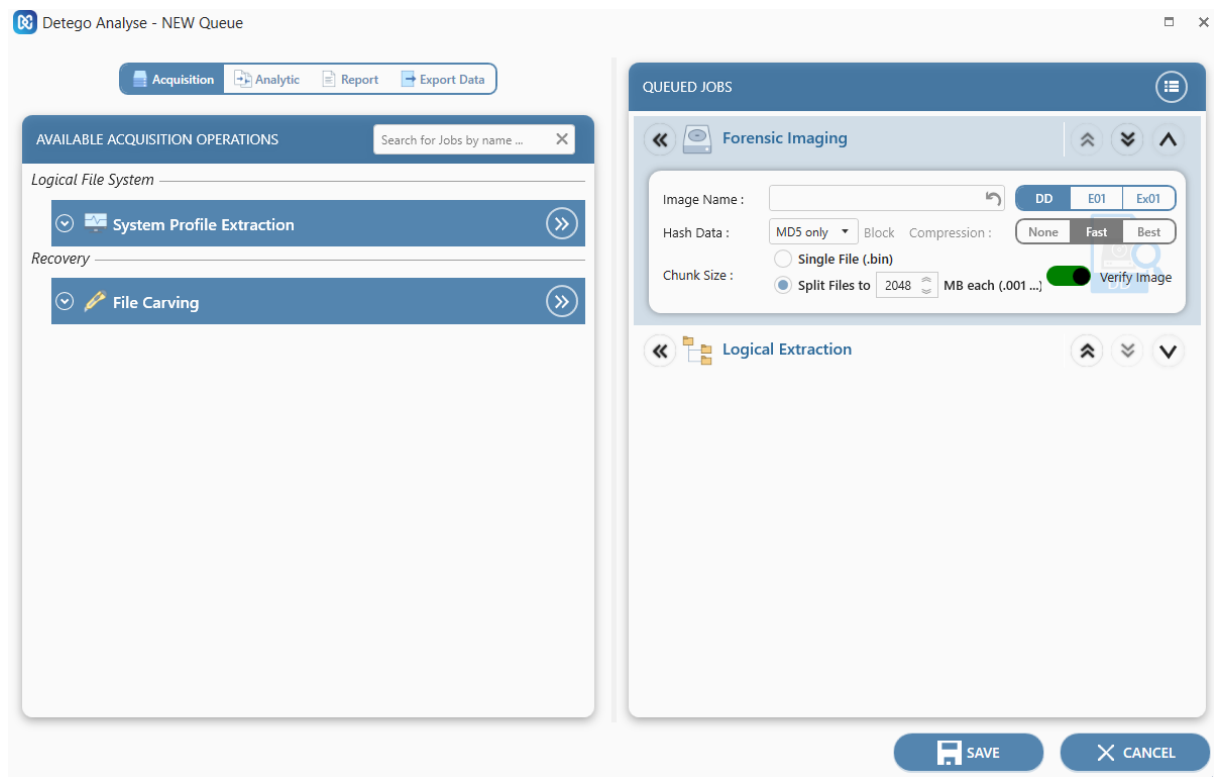
- Select the 'Job Queues' tab from the left panel in the CONFIGURATION cog
- Select the 'NEW QUEUE...' button from the bottom right corner of the window.

Figure 43



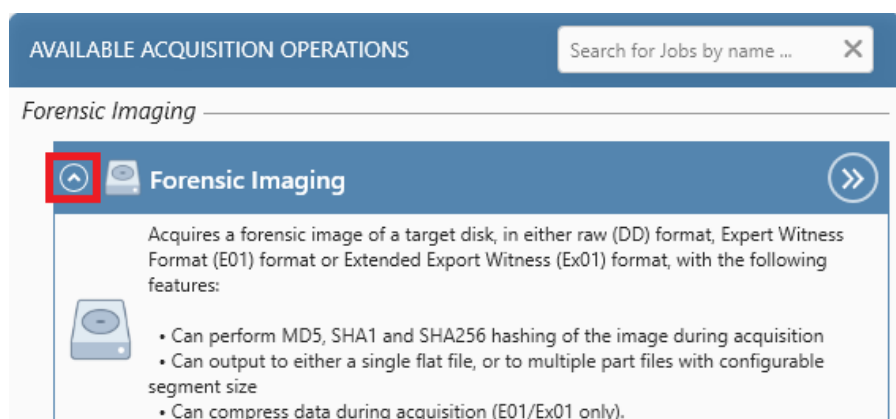
- From the 'New Job Queue' window, select the (>>) buttons on the right side of the jobs you wish to add, moving those jobs to the right panel under 'QUEUED JOBS'. To remove the jobs and move them back to the left panel, select the (<<) buttons. Selecting the dropdown buttons will display more options and details for the job.

Figure 44



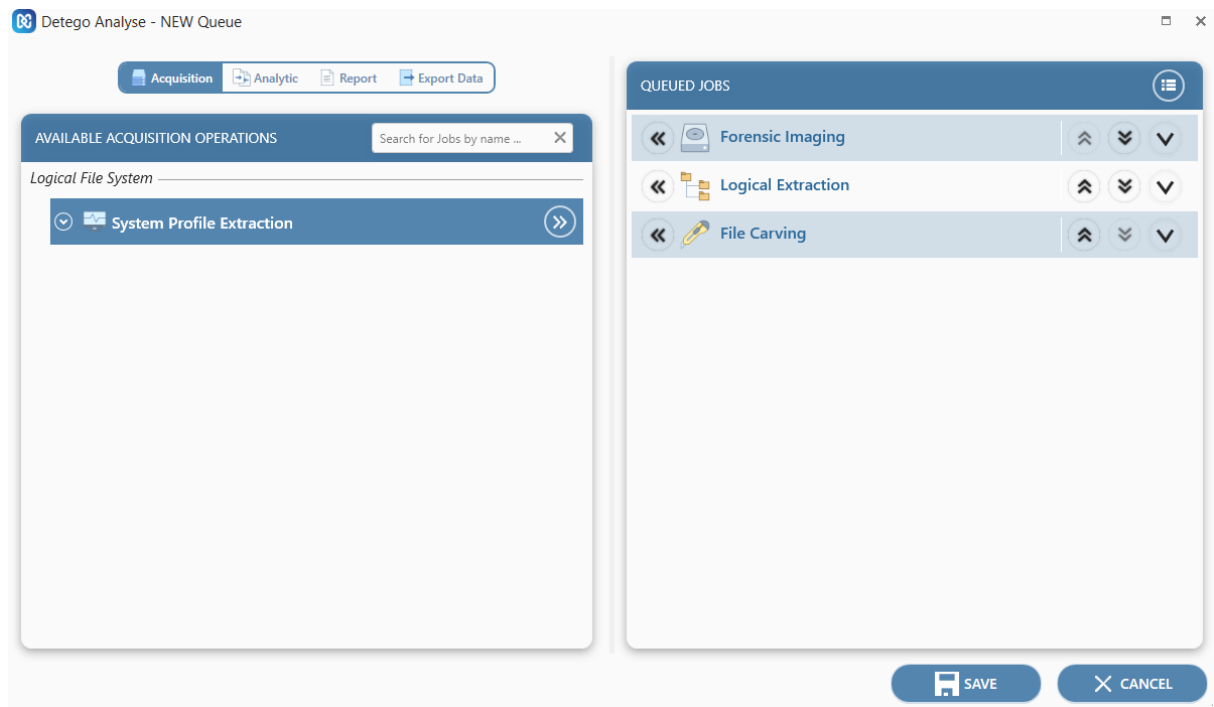
- Select the down arrow next to each title to learn more about the different types of data acquisition. In-depth details for all jobs are later in this guide.

Figure 45



Note: You can add multiple acquisition operations to the queue before defining other analytical processes.

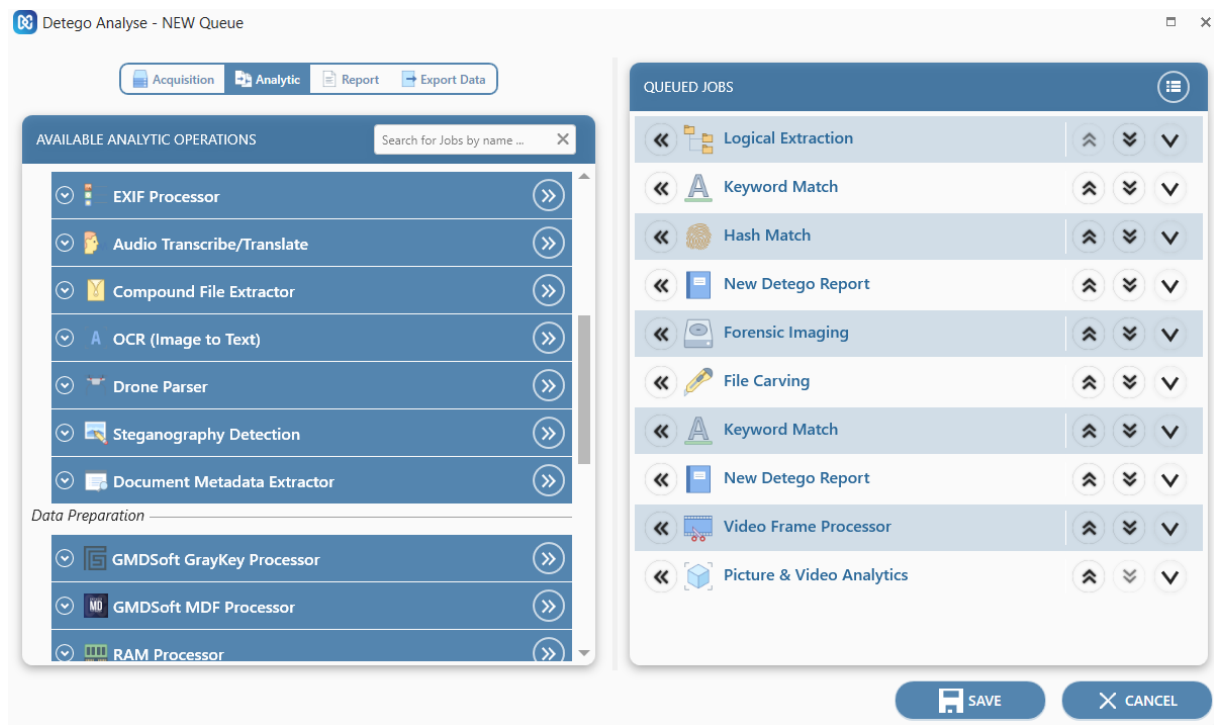
Figure 46



In the above example, we can see three jobs lined up. These will run sequentially with the Forensic Imaging, followed by a Logical Extraction and then File Carving.

- To add new processes, reports or exports to your job queue, click between the task tabs at the top of the left panel in the window and select the (>>) arrows on the processes and jobs you want to add. You can position each one as you wish in the sequence using the arrow controls to move each job up and down the list. Alternatively, a drag-and-drop feature allows you to click and hold a job and drag it anywhere in the queue to reposition it.

Figure 47

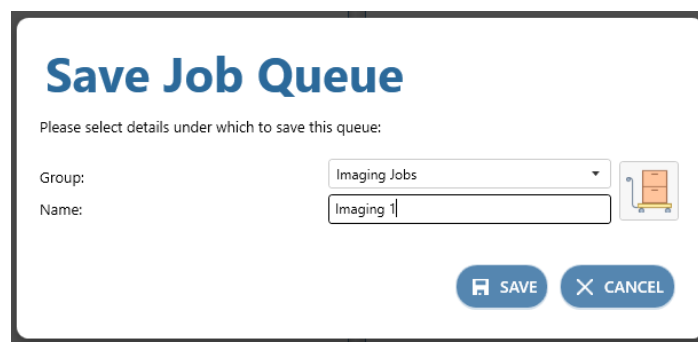


The finished job queue above follows a fairly common investigative workflow. In this scenario, the investigator has set up a workflow that completes a rapid logical extraction of their exhibit and then runs some critical keywords and hashlists against the dataset.

The workflow has been designed to give the investigator a series of 'quick wins' in minutes before the automated job queue moves on to the more time-consuming imaging processes, carving for deleted data and other analytical processes.

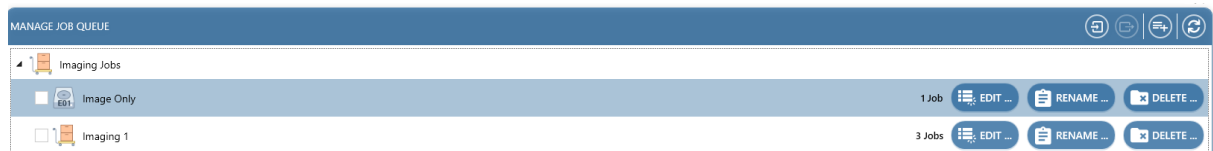
Once you are happy with your job queue, select the SAVE button at the bottom of the window and then name the Job Queue Group or select one from the list and name your Job Queue. You can also set the icon to associate with your job queue.

Figure 48



Once saved, the job queue will appear in the Job Queue window under the Job Queue Group.

Figure 49

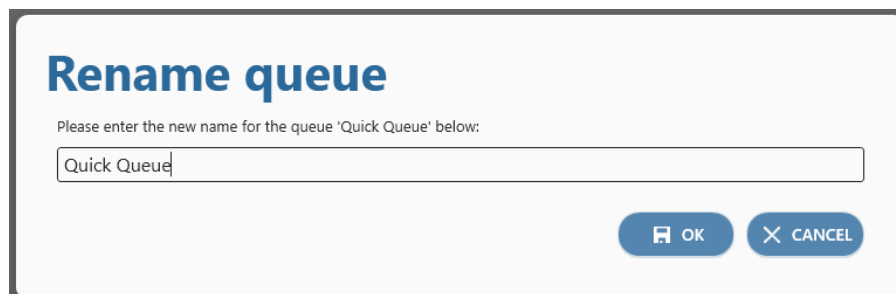


EDIT/RENAME/DELETE A JOB QUEUE

Once you have created and saved your job queues, you can select the EDIT, RENAME or DELETE buttons on the right side of the job queue.

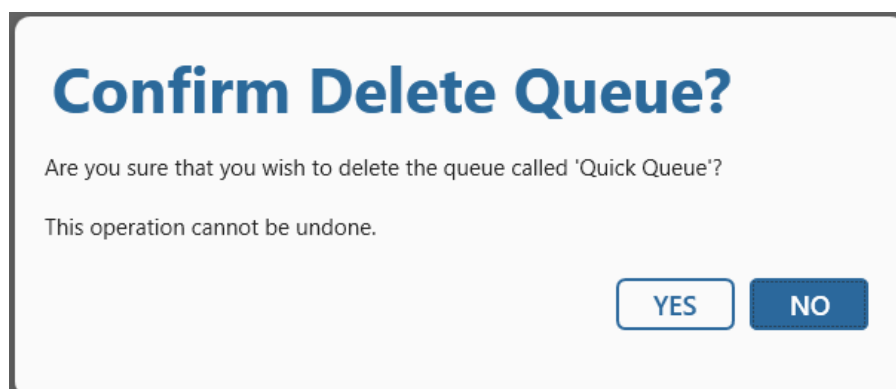
- Selecting the EDIT button allows you to reconfigure the jobs within the job queue.
- Selecting the RENAME button allows you to rename the job queue. Type the name you wish to rename and select OK to save the new name or Cancel to cancel the operation.

Figure 50



- Selecting the DELETE button allows you to delete the job queue. You will receive a prompt to confirm that you wish to delete it.

Figure 51

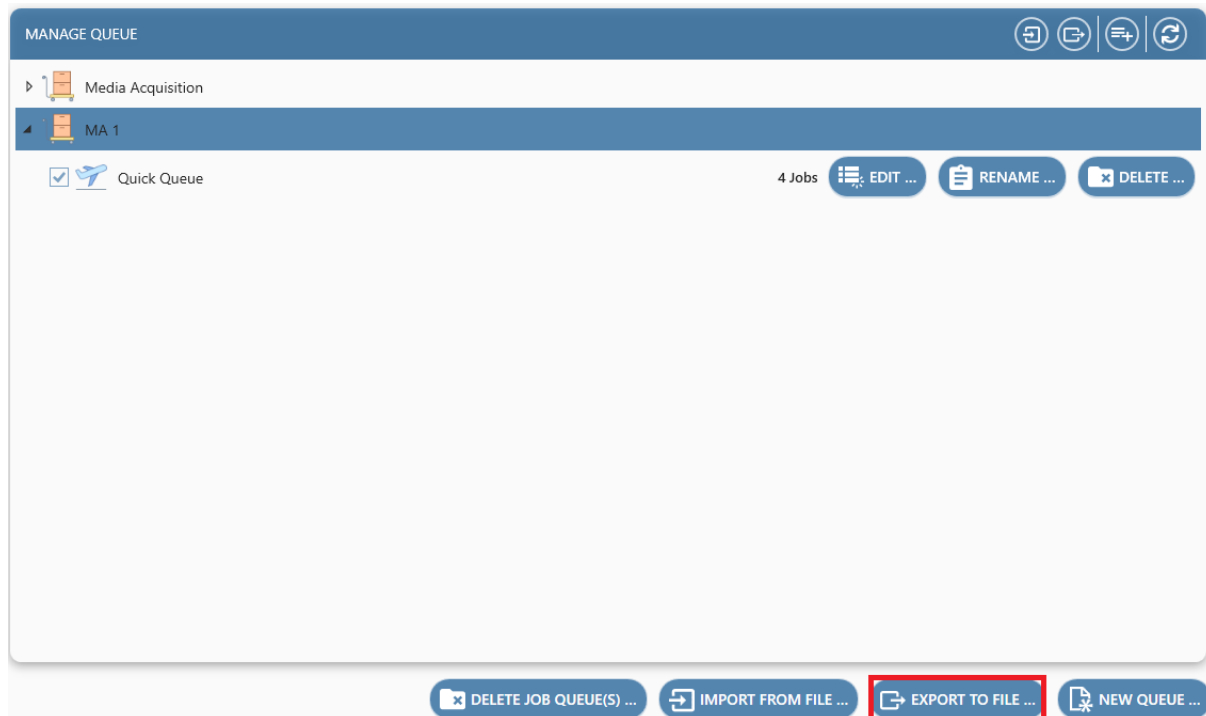


EXPORT A JOB QUEUE

To export a job queue, follow the below steps:

- Select the checkbox on the job queue(s) you wish to export and select the EXPORT TO FILE button in the bottom right corner.

Figure 52



- Save the 'DetegoSavedQueues...' file (.detegoqueue) to a location on your machine or device.
- Once saved, the below pop-up will be displayed as confirmation. Select OK.

Figure 53

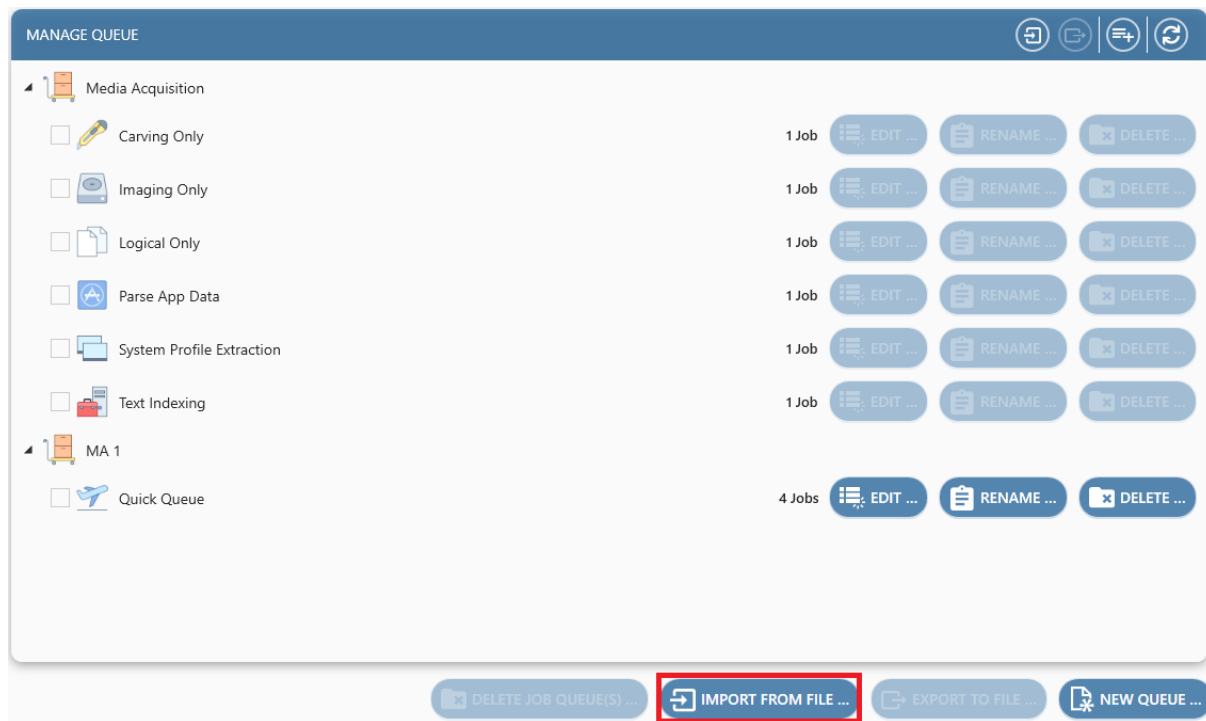


IMPORT JOB QUEUES

To import a job queue, follow the below steps:

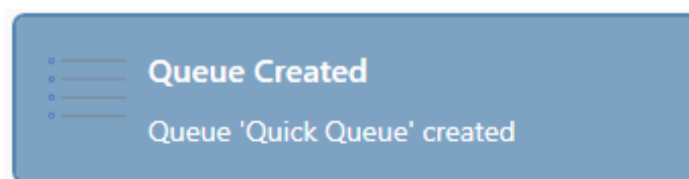
- Select the 'IMPORT FROM FILE...' button in the bottom right corner.

Figure 54



- Select the 'DetegoSavedQueues...' file (.detegoqueue) from wherever you have saved it on your machine/device and select Open.
- Once imported, the job will appear in the list, and a message will appear in the screen's bottom left corner saying successful.

Figure 55



3.4. CONFIGURING HASHLISTS

A hash is a unique hexadecimal identifier, displayed as a set of numbers and letters and assigned to an image or a file. Similar to a fingerprint, it's incredibly unlikely that two files containing different content would ever generate the same hash, helping to identify, verify and authenticate electronic evidence.

The process of hash matching works by importing a list of hashes connected to files containing

suspect material into Detego Analyse and comparing them against the acquired files stored within the software; any common matches will then be flagged.

Note: Before creating a hashlist, a text (.txt) file containing the line-separated hashes should be created for import. Hashes can be MD5 and SHA1. You can also manually import a hash without needing a .txt file.

Figure 56

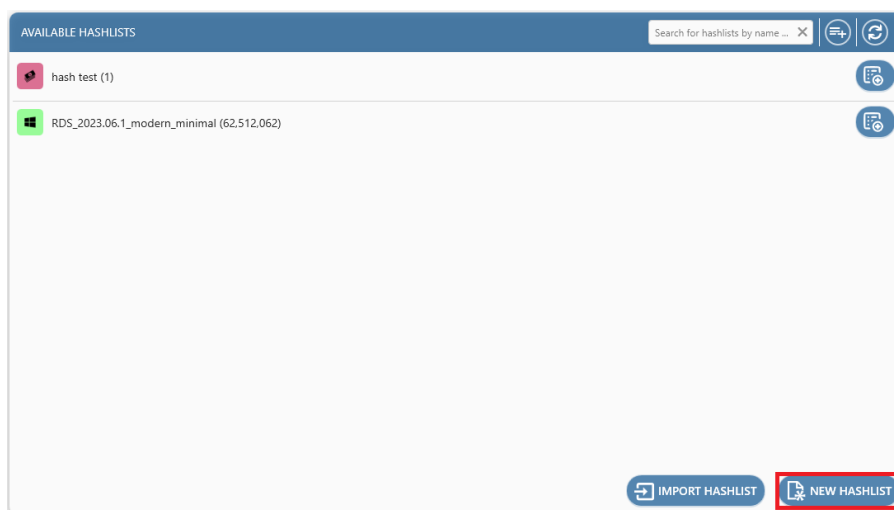
Hashlists

CREATING A NEW HASHLIST

To create a new Hashlist, follow the below steps:

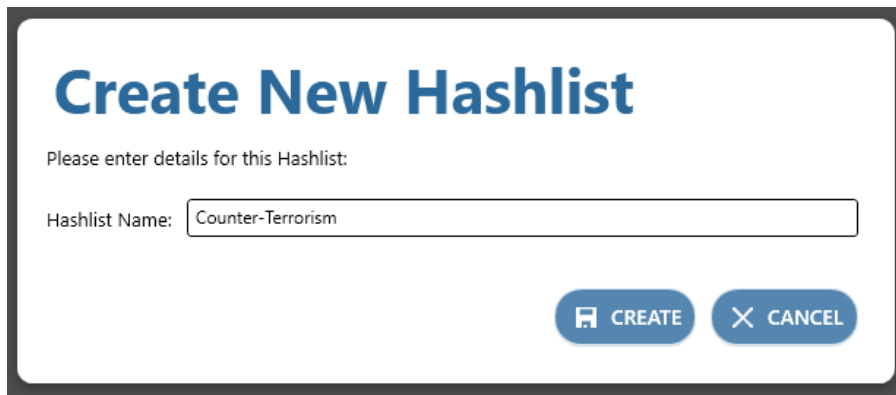
- Click on the 'NEW HASLIST' button in the bottom right corner of the window.

Figure 57



- In the 'New Hashlist' pop-up, enter a name for your new list and click 'OK' to save.

Figure 58

A dialog box titled "Create New Hashlist" in a large, bold, blue font. Below the title, it says "Please enter details for this Hashlist:". There is a text input field labeled "Hashlist Name:" with the text "Counter-Terrorism" entered. At the bottom right, there are two buttons: "CREATE" with a plus icon and "CANCEL" with an X icon.

Create New Hashlist

Please enter details for this Hashlist:

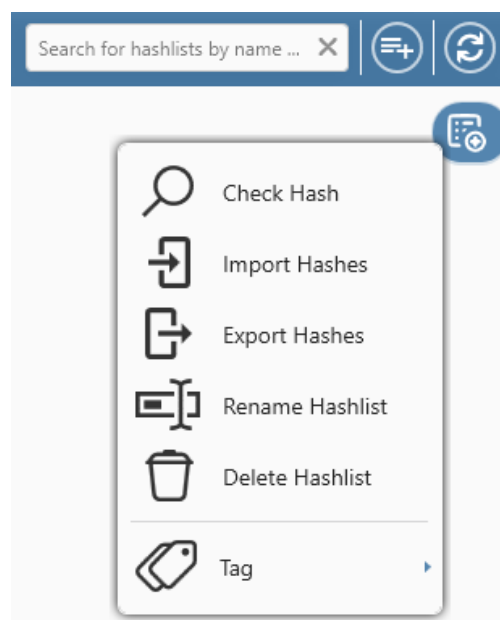
Hashlist Name:

CREATE **CANCEL**

MANAGING A HASHLIST

Clicking on the "MANAGE" button alongside your selected hashlist presents you with various options you can use to manage your hashlists.

Figure 59

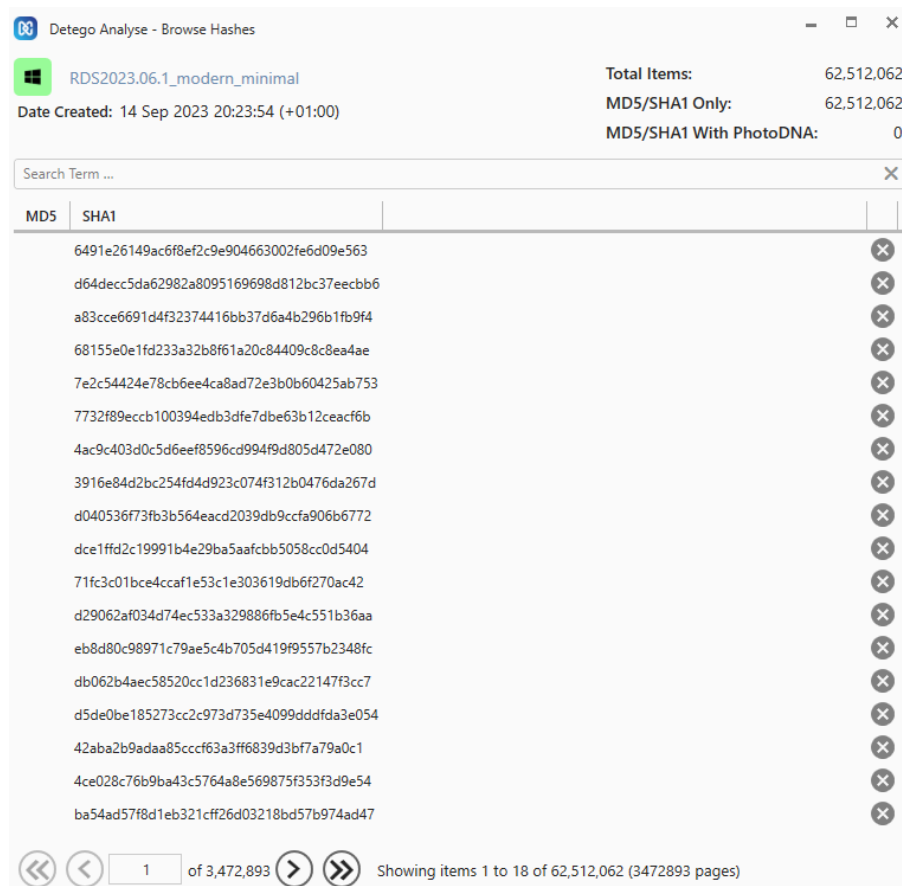


CHECK HASH

- Check Hash displays a list of all imported hashes. From here, the investigator can search for a particular hash, remove individual hashes, and view photo DNA hashes.
 - Select 'Check Hash' from the list of options.

- Enter the hash value into the search bar at the top of the 'Detego Analyse – Browse Hashes' window to find a particular hash. An appropriate message will be displayed if it's not in the system.
- You can remove an individual hash by clicking the 'X' icon next to it.
- Click on the navigation icons at the bottom of the window to navigate the pages if required.

Figure 60



IMPORT HASHES

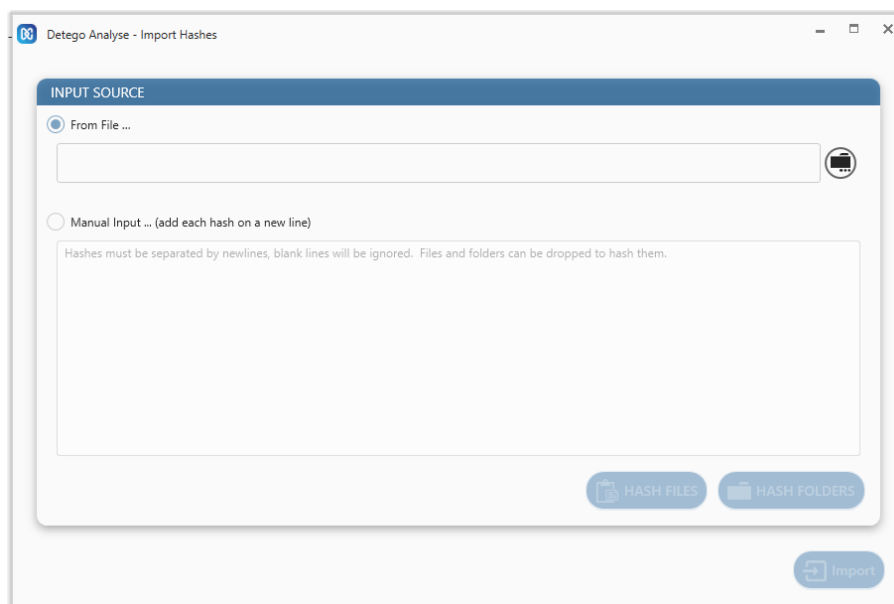
The operator can either import hashes from a file, i.e., a line-separated .txt file or manually, whereby the hashes are manually typed. Separate each hash by placing it on a new line. You can also drag and drop files and folders to hash them.

HASH FILES – This button allows you to browse and select a specific file to add its MD5 and SHA1 hashes to the list.

HASH FOLDERS – This button allows you to browse and select a specific folder to add the MD5 and SHA1 hashes of all the files in the list.

- Select the 'Import Hashes' option from the list of options.
- Select the radio button from the 'Detego Analyse – Import Hashes' window for your preferred option (either 'From File...' or 'Manual Input...').
- If the hashlist is a Project VIC file, two more options will be displayed. Please see the Project VIC section for more information.

Figure 61



- If the import is successful, a message will display in the bottom left corner showing the number of hashes imported (any duplications are ignored).

NOTE! If you want to import a hashlist instead of creating a new one and importing into that, please select the IMPORT HASHLIST button in the bottom right corner of the screen.

Within the Evidence Browser, you can add existing hashlists or create new hashlists from a chosen selection.

EXPORT HASHES

This function exports a hashlist into a Detego Hashlist Database (.dhd) file, used on another instance or later.

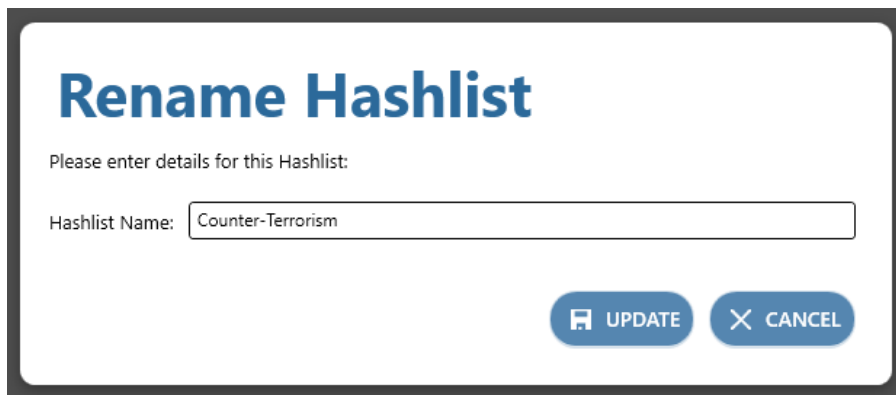
- Select the 'Export Hashes' option from the list.
- Save the file to a location on your device.

RENAME HASHLIST

From here, the investigator can change the name of a particular hashlist.

- Select 'Rename Hashlist' from the list.
- Input the name you would like to change the Hashlist to.
- Select UPDATE to rename the Hashlist.

Figure 62



Rename Hashlist

Please enter details for this Hashlist:

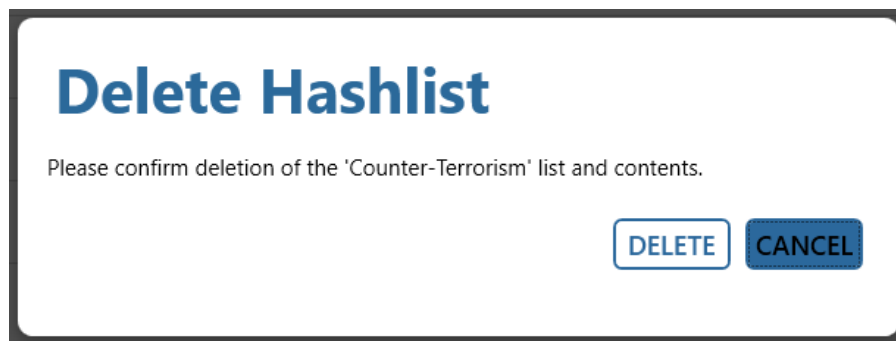
Hashlist Name:

DELETE HASHLIST

This function removes the Hashlist from Detego Analyse.

- Select the 'Delete Hashlist' option from the list.
- Select the DELETE button in the confirmation prompt to complete deletion or select CANCEL to cancel the task.

Figure 63

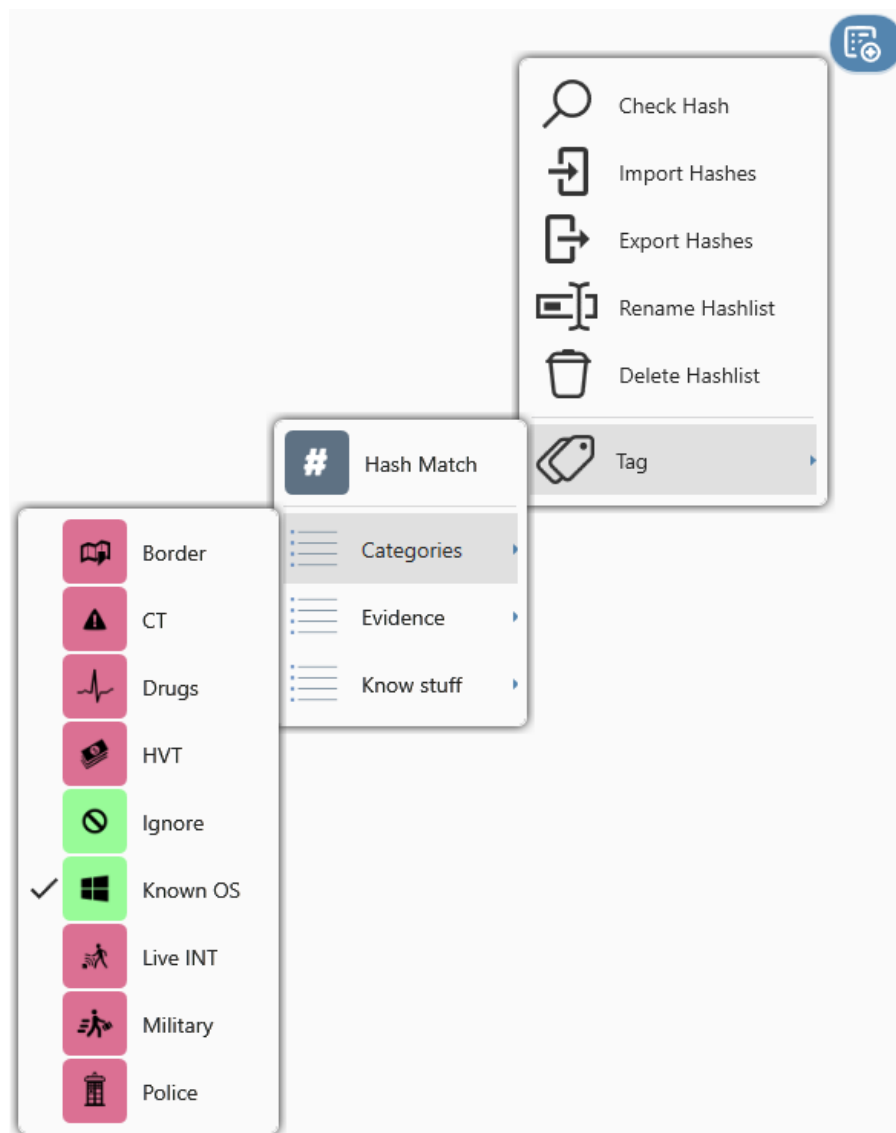


TAG

This function allows you to set the tag type applied to each hash match.

- Select the 'Tag' option from the list and select your desired tag from the dropdown menu.

Figure 64



ADDING NSRL/HASH REJECTION LISTS

An NSRL (National Software Reference Library) list contains the hashes of common, known safe software files such as Windows system files. Lists can be added to Detego so that its extraction tools can safely avoid extracting unnecessary files.

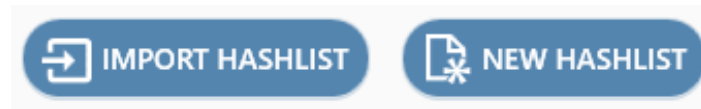
NOTE! If you have access to the Detego Installation Manager, you can download and install the latest converted NSRL/Hash Rejection list. Doing so will automatically apply the correct tags to this for use within Detego Analyse and Detego Field and therefore the below steps do not need to be followed.

Also note that any Rejection lists must be in .csv or .txt format.

Please follow the below steps to add an NSRL/Hash Rejection List manually:

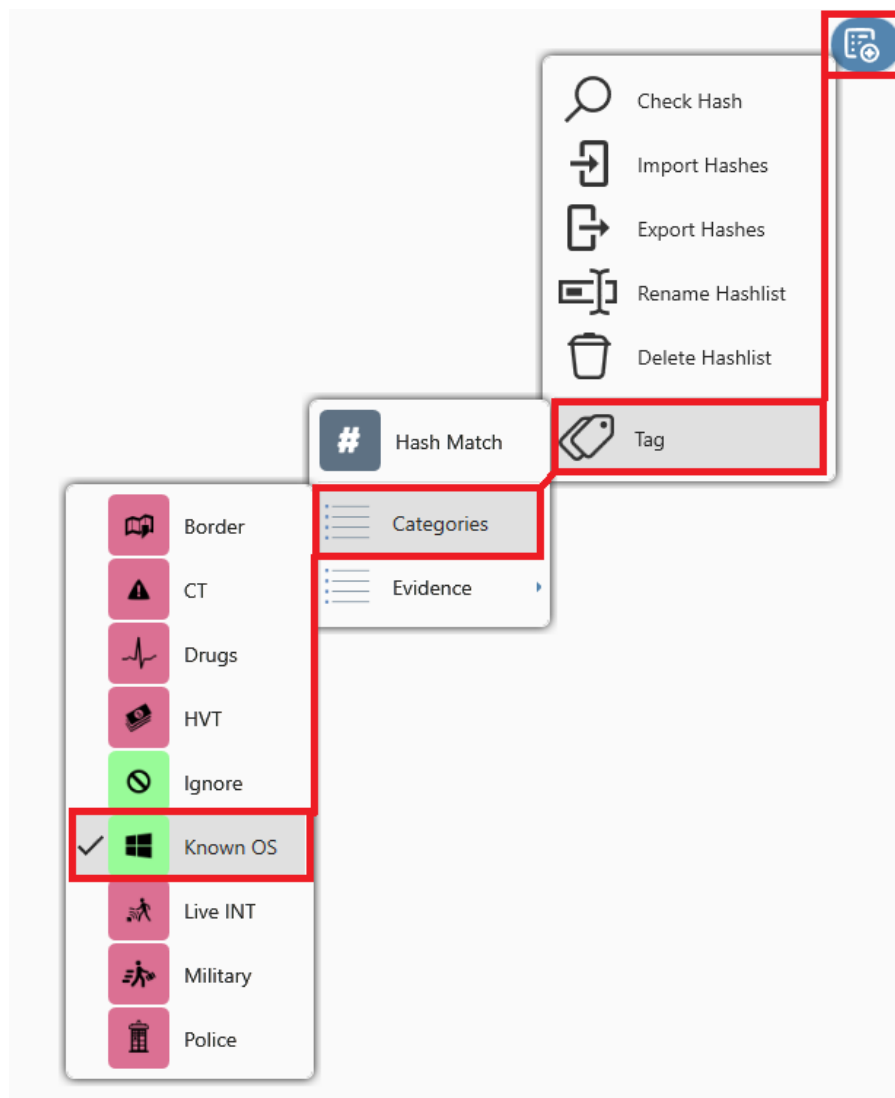
- Select the 'New Hashlist' button to create a new Hashlist or if you already have a .dhd of an existing hashlist, select the 'Import Hashlist' button.

Figure 65



- If not already done so, import the correct hashes into your Hashlist.
- Once the hashes have been imported, select the Context Menu button for the Hashlist and select 'Tag > Categories > Known OS'

Figure 66



Tagging as Known OS will mark the item/hashlist as safe and can be added to Detego Field for further functionality.

PROJECT VIC HASHLIST

Detego Analyse supports Project VIC Hashlists. This includes the handling of mandated Project VIC format (Base64 format), Project VIC categorisation and exportation into the correct format handled by Project VIC.

PLEASE NOTE! You must have access to Project VIC to utilise this functionality.

IMPORTING A PROJECT VIC HASHLIST

To import a Project VIC Hashlist, please follow the below steps:

- Create a new blank hashlist and browse for the file as usual. Details on creating hashlists can be found in the Creating a New Hashlist section.
- Select the 'Import Hashes' option from the "MANAGE" button menu for the new hashlist.
- Browse for the Project VIC file to import to your hashlist. Detego Analyse will automatically detect the Project VIC format, and the 'Project VIC Option' section will be displayed. An error message will be displayed if the file is not in the correct Project VIC format.

Figure 67

Detego Analyse - Import Hashes

INPUT SOURCE

☒ From File ...

C:\Users\Alex.MCMS\Downloads\Photo_DNA_testdata\1mil_PV_hash.json

Project VIC Options

Category Tag Groups: New... Available Category Files: United Kingdom

Import as: Project VIC Categories - United Kingdom

☒ Include Ignorable

☐ Manual Input ... (add each hash on a new line)

Hashes must be separated by newlines, blank lines will be ignored. Files and folders can be dropped to hash them.

HASH FILES HASH FOLDERS

Import

- If the Project VIC format is detected, additional fields are provided to select the tag group to map the Project VIC category number to an Analyse tag. Existing Project VIC tag groups are provided in a combo box and a 'New...' option. Only tag groups marked with the Project VIC flag will be available for selection.
- If a new source is selected, two further controls are displayed. These are the 'Available Category Files' option and the 'Import as' textbox. The first allows you to select a format file from the '%PROGRAMDATA%/Detego/Project VIC' folder. Any files detected will be loaded into the combo box, and the user can then change the name in the textbox to name a new tag group.
- The Include Ignorable Toggle allows you to select whether ignorable tags are imported or not.
- Once the import has begun, the tag group will be marked against the hashlist and cannot be changed on subsequent imports. The group will be displayed in the combo box but will be disabled.

- Wait for the import process to complete. Once completed, you'll notice that the hashlist will have the Project VIC flag applied to it.

Figure 68

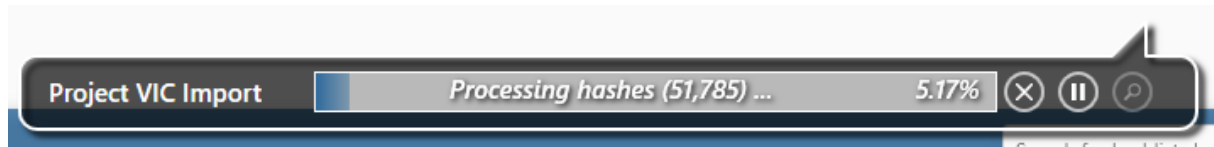
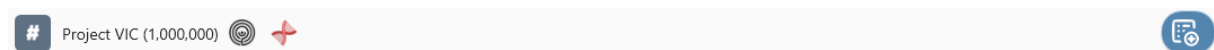


Figure 69

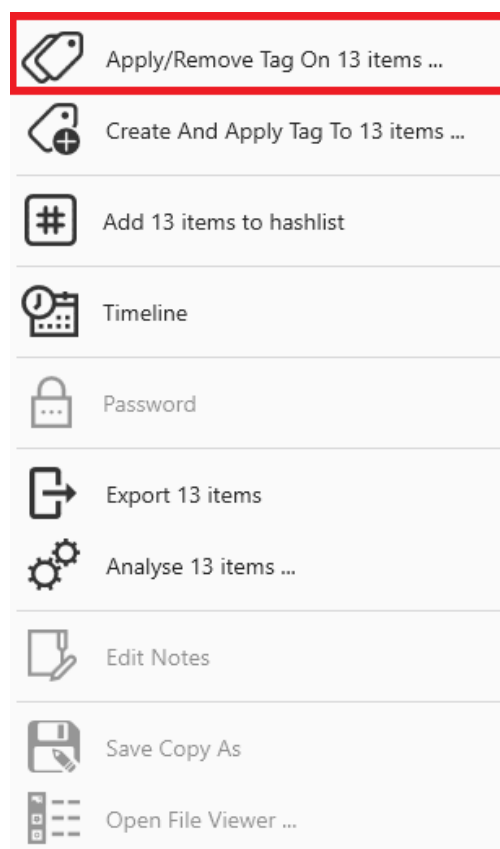


TAGGING FOR PROJECT VIC

To add a Project VIC tag to an untagged item, follow the below steps:

- Navigate to the Evidence Browser and locate the item(s) you wish to tag with the Project VIC tag.
- Select the items and right click on one of them, select 'Apply/Remove Tag on X items ...' and select the Project VIC options you wish to apply.

Figure 70

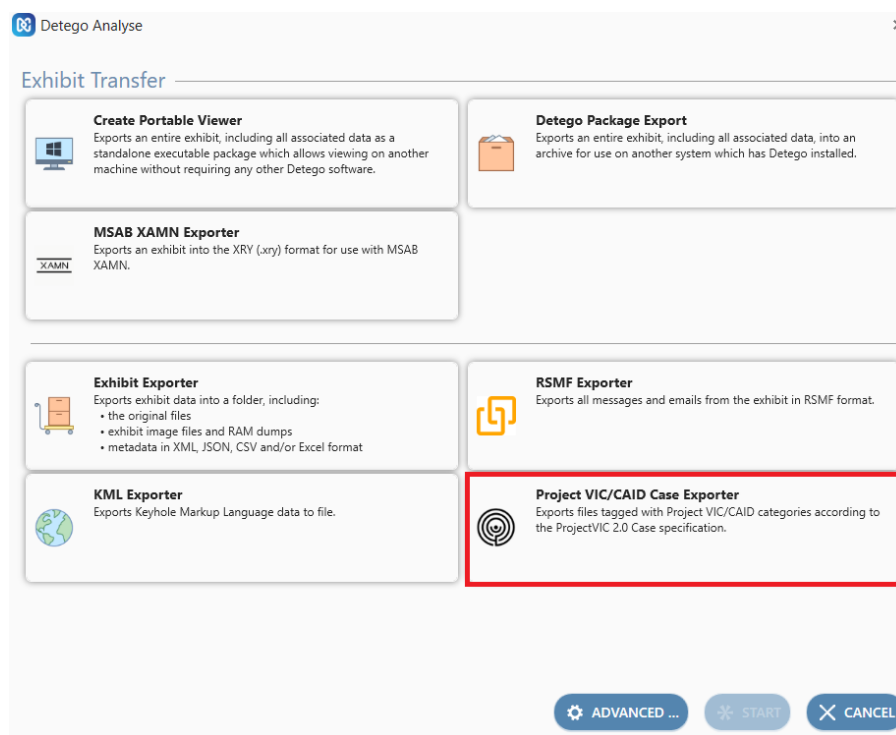


PROJECT VIC TAGGED IMAGE HASH EXPORTER

To export Project VIC Tagged Image Hashes, follow the below steps:

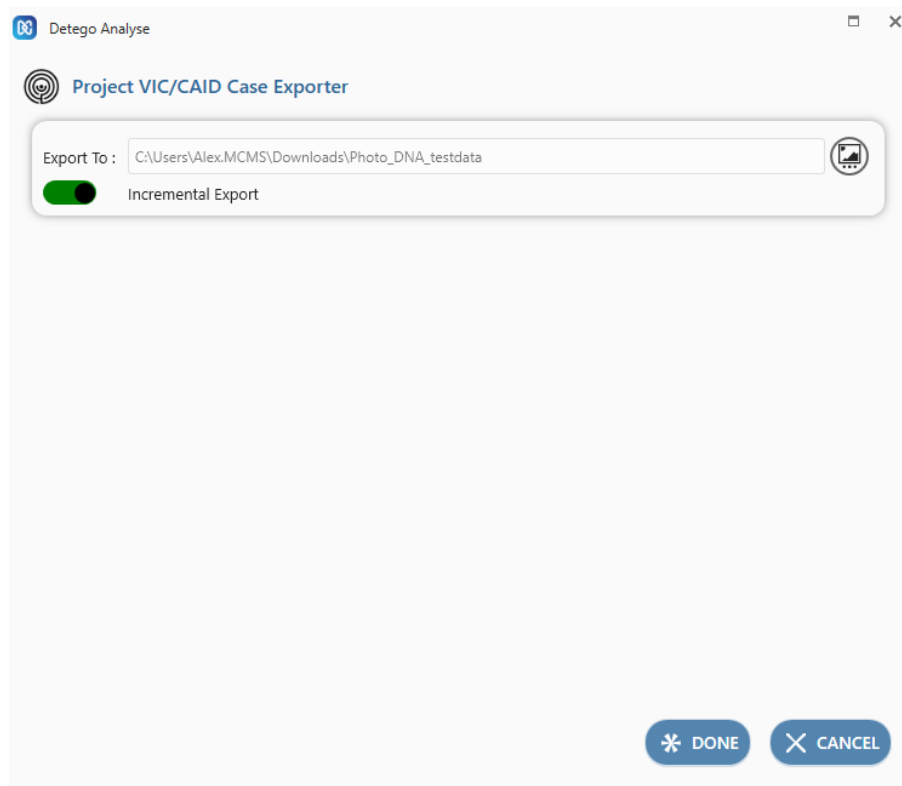
- Select the exhibit you wish to export the Project VIC-tagged items from.
- Select the 'Export' button in the bottom right corner.
- Select the 'Project VIC/CAID Case Exporter' job.

Figure 71



- Select a location to save the file and toggle on or off whether you wish to do an incremental export.
 - Incremental export will export only images that have not been previously exported to Project VIC.

Figure 72



3.5. CONFIGURING FACE WATCHLISTS

Face Watchlists and a face recognition job are possible within Detego Analyse. They follow a similar design to hashlists and keyword lists.

Figure 73

Face Watchlists

To perform face recognition, the following steps must be followed:

- Create a new face watchlist
- Import faces into the face watchlist
- Run the visual indexer job on an exhibit
- Run the face recognition job on an exhibit
- View the results as tags

CREATING A NEW FACE WATCHLIST

To create a new Face Watchlist, follow the below steps:

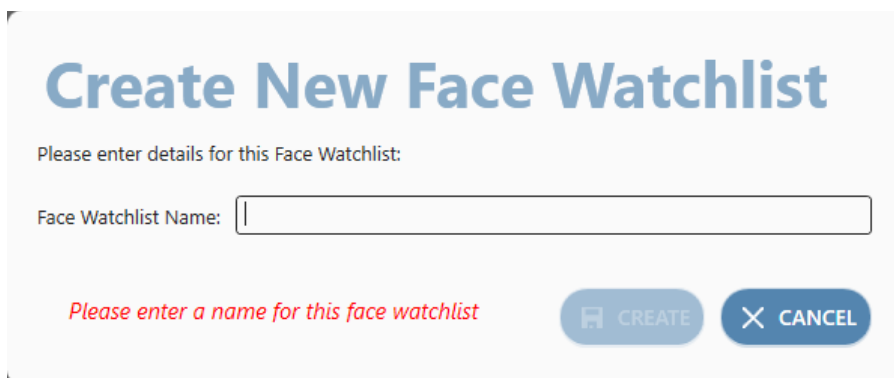
- From the Face Watchlist screen, select the 'NEW FACE WATCHLIST' button in the bottom right corner.

Figure 74



- Type in the Face Watchlist name and then select the 'CREATE' button.

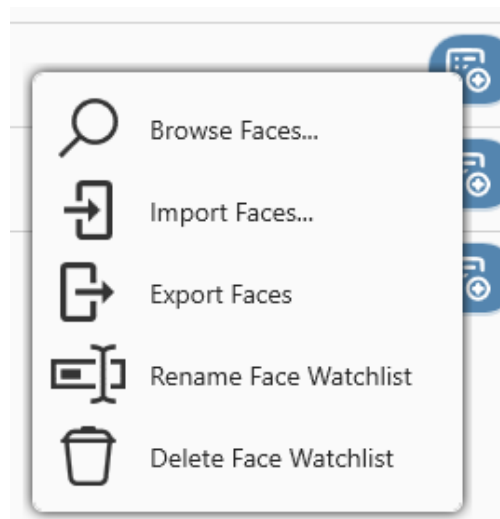
Figure 75

A screenshot of a 'Create New Face Watchlist' form. At the top, the title 'Create New Face Watchlist' is displayed in a large blue font. Below the title, a smaller text prompt says 'Please enter details for this Face Watchlist:'. This is followed by a text input field with the label 'Face Watchlist Name:'. Below the input field, a red error message reads 'Please enter a name for this face watchlist'. At the bottom right of the form, there are two buttons: a light blue 'CREATE' button and a dark blue 'CANCEL' button.

Once you have created the new Face Watchlist, you will need to import Faces before you can use it. You can also perform on a Face Watchlist, the below actions:

- Browse Faces
- Import Faces
- Export Faces
- Rename Face Watchlist
- Delete Face Watchlist

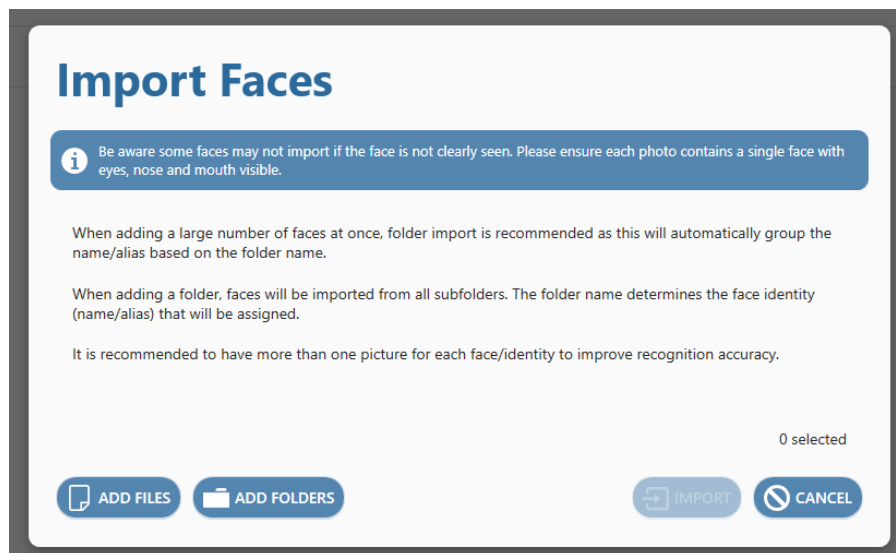
Figure 76



IMPORTING INTO A FACE WATCHLIST

Select the import faces function from the Face Watchlist context menu.

Figure 77



An example folder structure when importing a folder of faces:

Faces Folder/

Mr_Smith/

— face1.jpg

— face2.jpg

Unknown_PersonA/

— face1.jpg

— face2.jpg

— face3.jpg

Unknown_PersonB/

— face1.jpg

— face2.jpg

In this example, three distinct identities are created and will be named as follows:

- Mr_Smith (2 pictures)
- Unknown_PersonA (3 pictures)
- Unknown_PersonB (2 pictures)

Any picture of a face being added to a face watchlist must be cropped correctly only to include one face. Having more than one picture of a face (in various poses and angles) is recommended and will improve face recognition accuracy.

Figure 78



You may rename a face in the face watchlist, but be careful, as the face's name must match *exactly* the other face pictures of the same person/identity.

CHECK, EXPORT, RENAME AND DELETE FACE WATCHLISTS

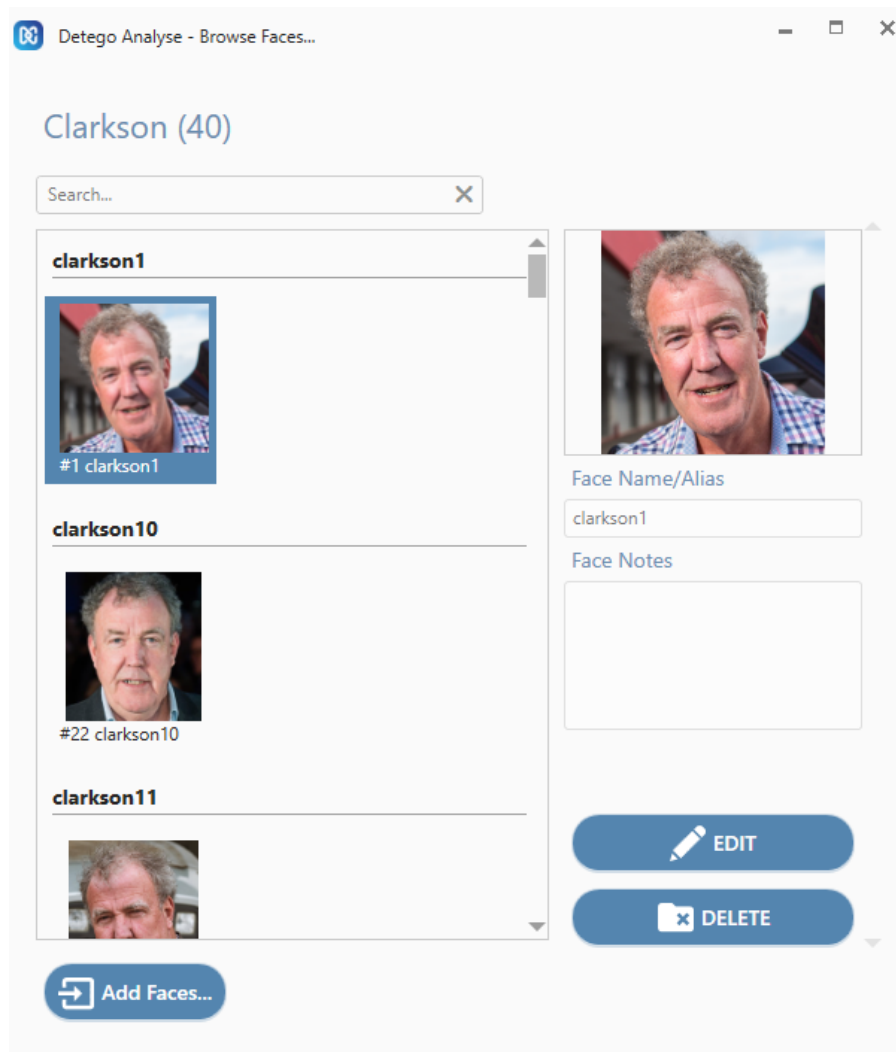
Using the Manage button on the Face Watchlist, you have several other options. These are:

- Check Faces
- Export Faces
- Rename Face Watchlist
- Delete Face Watchlist

CHECK FACES

- Select Check Faces option from the Manage button and the below screen will appear with a list of your faces.
- When you select a Face from the list, it displays the name of the Face and any Face Notes that may have been added. You can rename the Face Name/Alias of each Face and add/change any notes by selecting the EDIT button and then making your changes.
- Once any changes are made, select the SAVE button to save your changes.
- Select delete if you wish to delete a Face from the list.
- You can also add Faces using the bottom left button.

Figure 79



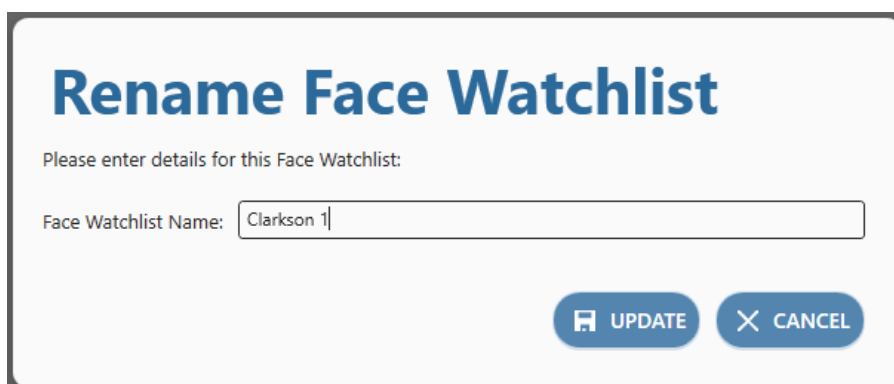
EXPORT FACES

- You can export a Face Watchlist by selecting the Manage button on your Face Watchlist
- Select 'Export Faces'.
- Save the Face Watchlist to a folder of your choice.

RENAME FACE WATCHLIST

- You can rename a Face Watchlist by selecting the Manage button on your Face Watchlist
- Select 'Rename Face Watchlist'.
- Input the new name for your Face Watchlist and select UPDATE.

Figure 80



Rename Face Watchlist

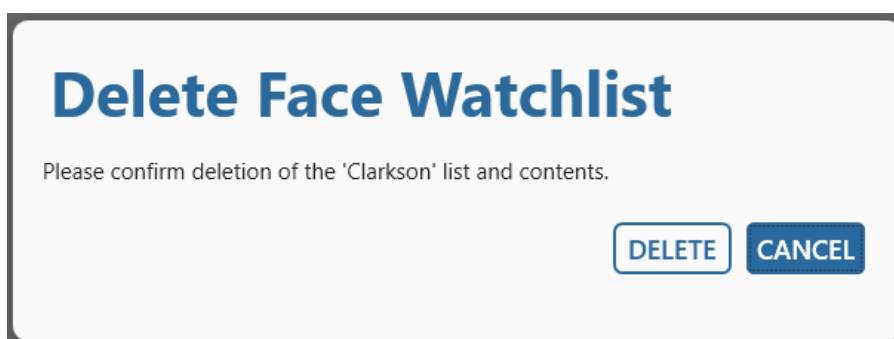
Please enter details for this Face Watchlist:

Face Watchlist Name:

DELETE FACE WATCHLIST

- You can delete a Face Watchlist by selecting the Manage button on your Face Watchlist
- Select 'Delete Face Watchlist'.
- Select DELETE to confirm deletion.

Figure 81



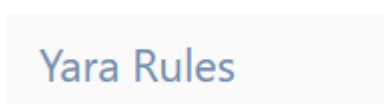
Delete Face Watchlist

Please confirm deletion of the 'Clarkson' list and contents.

3.6. CONFIGURING YARA RULES

Detego Analyse has a malware detection based on the Yara project. Yara works on the basis of rules that describe arbitrary data patterns, in our case patterns that can indicate malware across files, memory or backup data.

Figure 82



CREATING A NEW YARA RULE SET

To create a new Yara Rule set, follow the steps below:

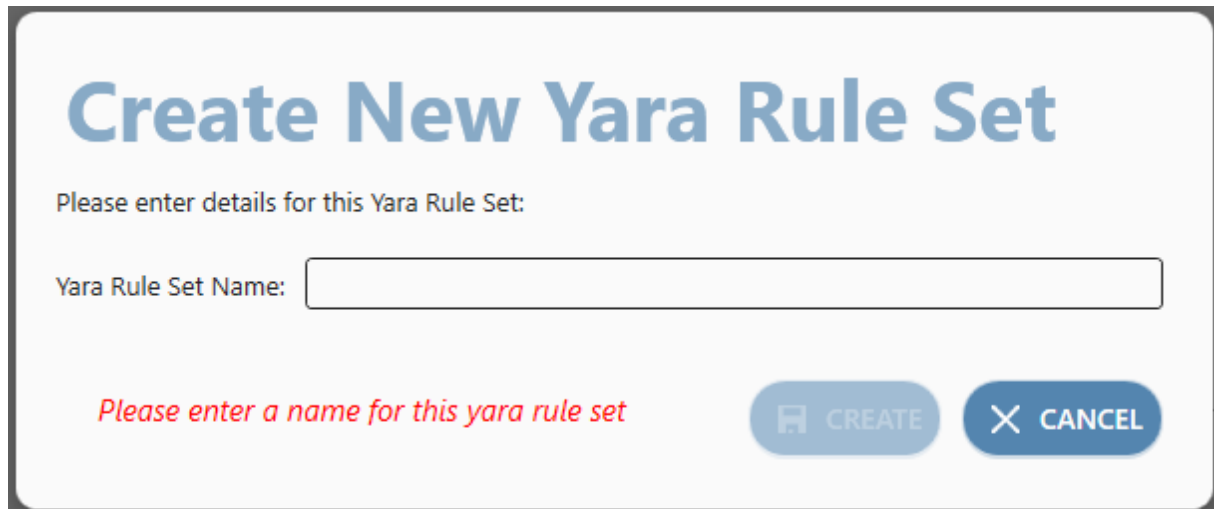
- Select the "NEW YARA RULE SET" button in the bottom right corner.

Figure 83



- Name your new rule set and select CREATE when ready.

Figure 84



Create New Yara Rule Set

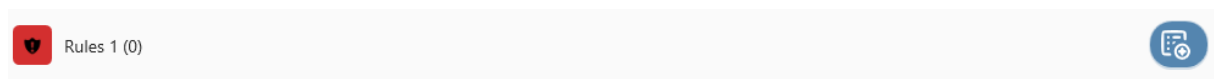
Please enter details for this Yara Rule Set:

Yara Rule Set Name:

Please enter a name for this yara rule set

Once created you will see something similar to the below:

Figure 85



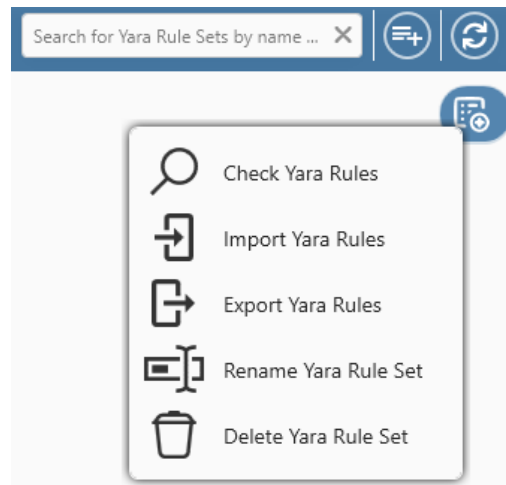
From here you can now manage the Rule Set from the MANAGE button (menu icon) on the right of each rule set.

MANAGING YARA RULE SETS

On the right side of a Rule Set, you can select the Manage button.

Clicking on the "MANAGE" button alongside your selected Yara Rule Set, presents you with various options you can use to manage your Yara Rule Sets.

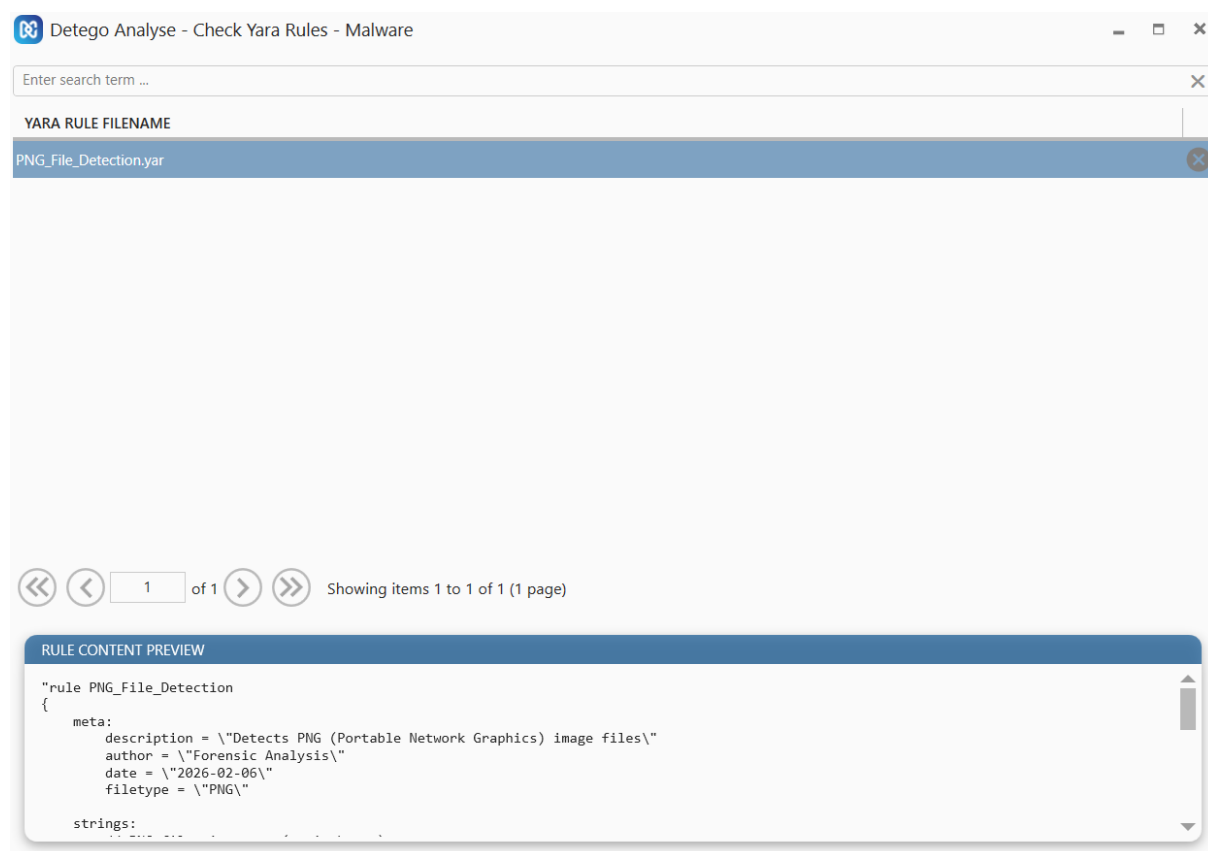
Figure 86



CHECK YARA RULES

- Check Yara Rules displays a list of all imported Yara Rules. From here, you can search, remove Rules and view each Rule's Content Preview.
 - Select 'Check Yara Rules' from the list of options.
 - Enter the term into the search bar at the top of the 'Detego Analyse – Check Yara Rules' window to find a particular term. An appropriate message will be displayed if it's not in the system.
 - You can remove an individual Yara Rule by clicking the 'X' icon next to it.
 - Click on the navigation icons at the bottom of the window to navigate the pages if required.
 - When selecting a rule, the Rule Content Preview will display at the bottom of the window allowing you to scroll through the content preview.

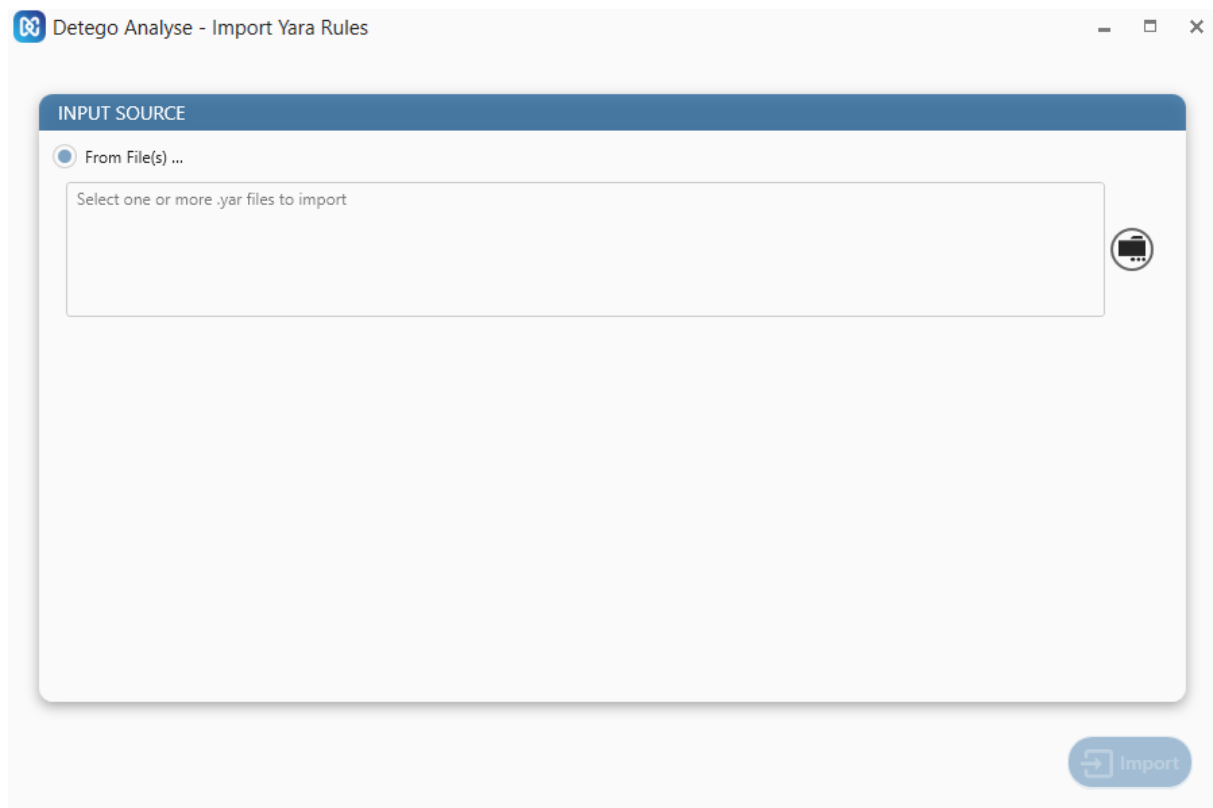
Figure 87



IMPORT YARA RULES

You can import Yara Rules from one of more .yar or .yara files.

Figure 88



- Select the 'Import Yara Rules' option from the list of options.
- Select the the BROWSE icon and then browse to the Yara files to import.
- Once you have selected your files, select the Import button to import them into your Rule Set.

EXPORT YARA RULES

This function exports a Yara Rules into a folder of your choice.

- Select the 'Export Yara Rules' option from the list.
- Save the file to a location on your device.

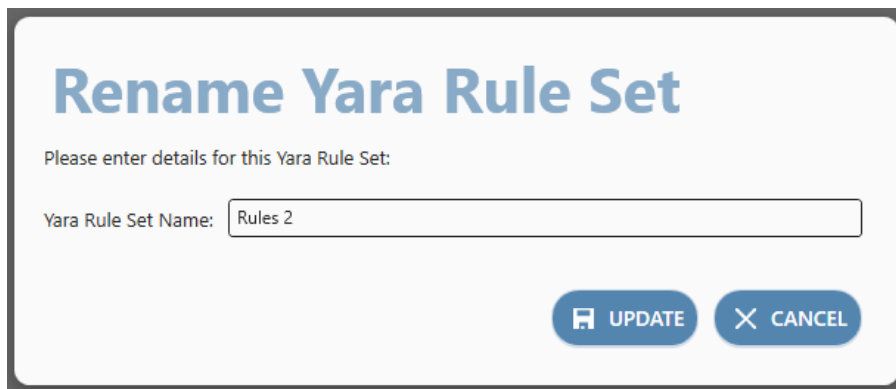
RENAME YARA RULE SET

From here, the investigator can change the name of a particular Yara Rule Set.

- Select 'Rename Yara Rule Set' from the list.
- Input the name you would like to change the Yara Rule Set to.

- Select UPDATE to rename the Yara Rule Set or CANCEL to cancel the operation.

Figure 89

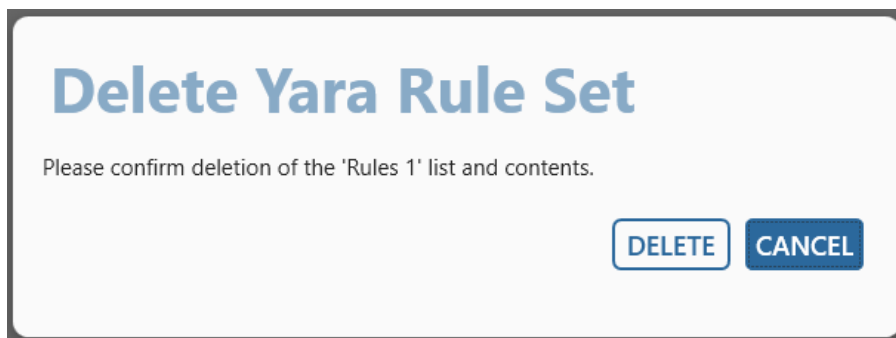
A dialog box titled "Rename Yara Rule Set" in a large blue font. Below the title, it says "Please enter details for this Yara Rule Set:". There is a text input field labeled "Yara Rule Set Name:" containing the text "Rules 2". At the bottom right, there are two buttons: "UPDATE" with a document icon and "CANCEL" with an 'X' icon.

DELETE YARA RULE SET

This function removes the Yara Rule Set from Detego Analyse.

- Select the 'Delete Yara Rule Set' option from the list.
- Select the DELETE button in the confirmation prompt to complete deletion or select CANCEL to cancel the task.

Figure 90

A dialog box titled "Delete Yara Rule Set" in a large blue font. Below the title, it says "Please confirm deletion of the 'Rules 1' list and contents.". At the bottom right, there are two buttons: "DELETE" and "CANCEL".

3.7. CONFIGURING FIELD PROFILES

The Field Profiles tab within Configuration settings allows you to harvest existing Field Profiles from ready-to-go Field devices. This allows creating a master Field Device with all the profiles you want and then harvesting them into Detego to license out to Field devices with them already created. This will save you time and effort and remove the need to set up all Field devices individually before sending them out.

Figure 91

Detego Field Profiles

HARVESTING DETEGO FIELD PROFILES

Detego Field Profiles have to be created on a Detego Field device and then “harvested” within Detego Analyse in order to license them out on other Detego Field devices.

In order to harvest profiles, follow the below steps:

- Navigate to the Field Devices tile from the HOME screen and insert your Field Device with the saved profiles.
- Select the 'PROFILES' button.

Figure 92

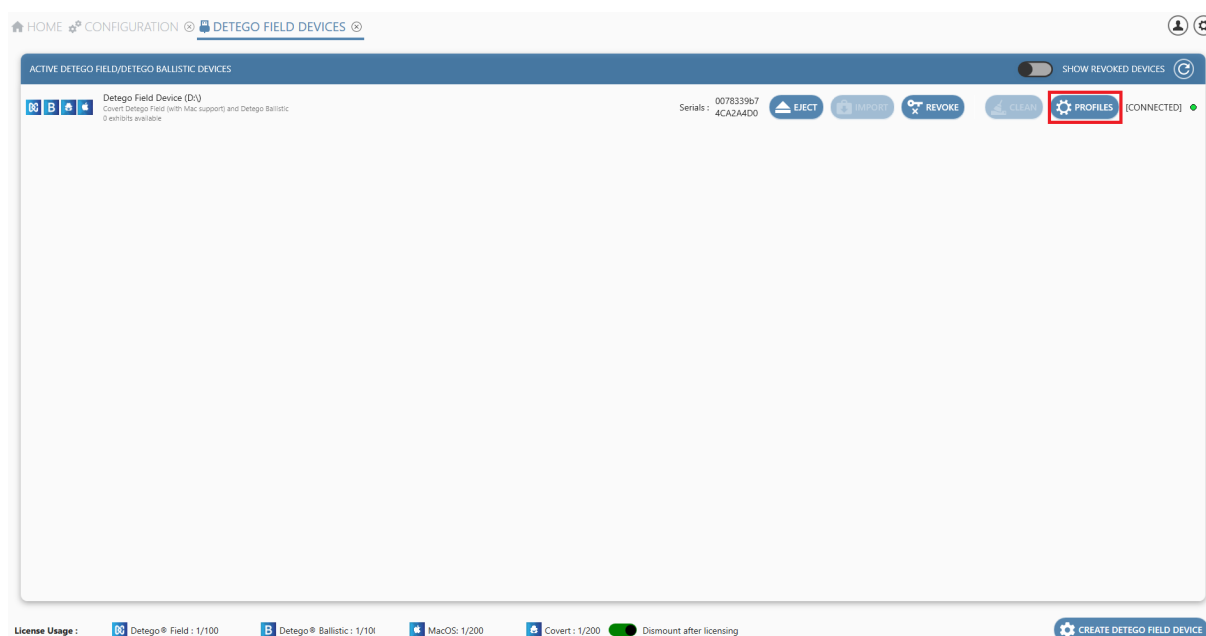
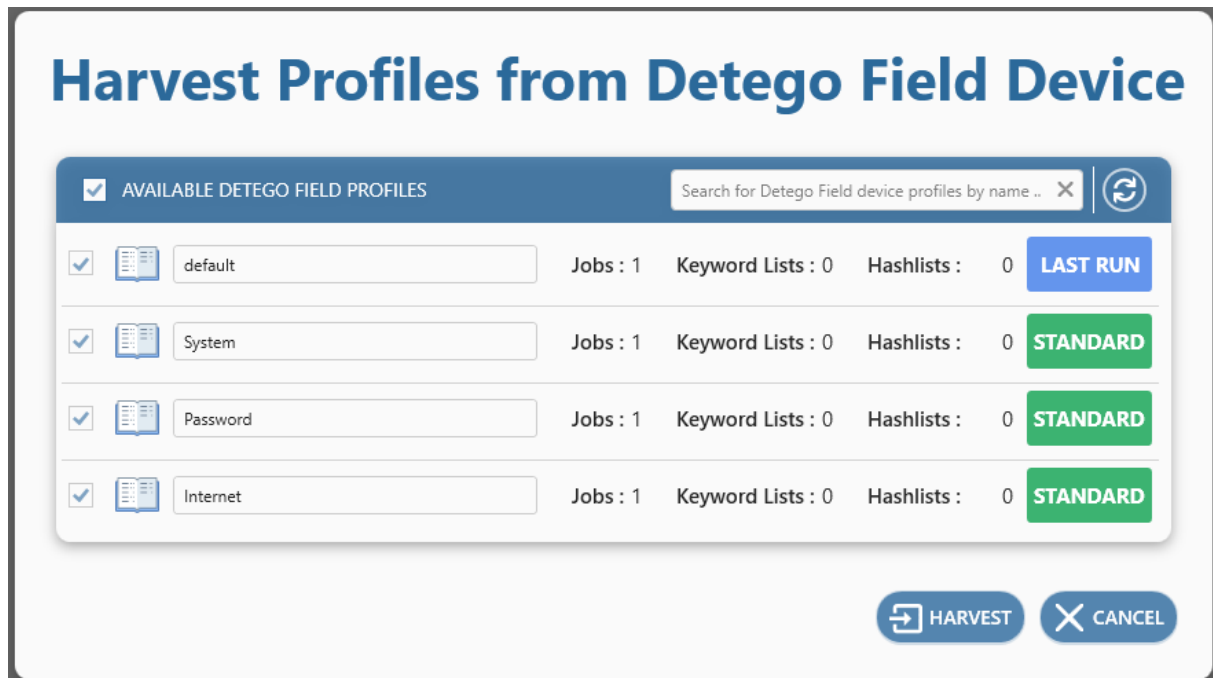


Figure 93

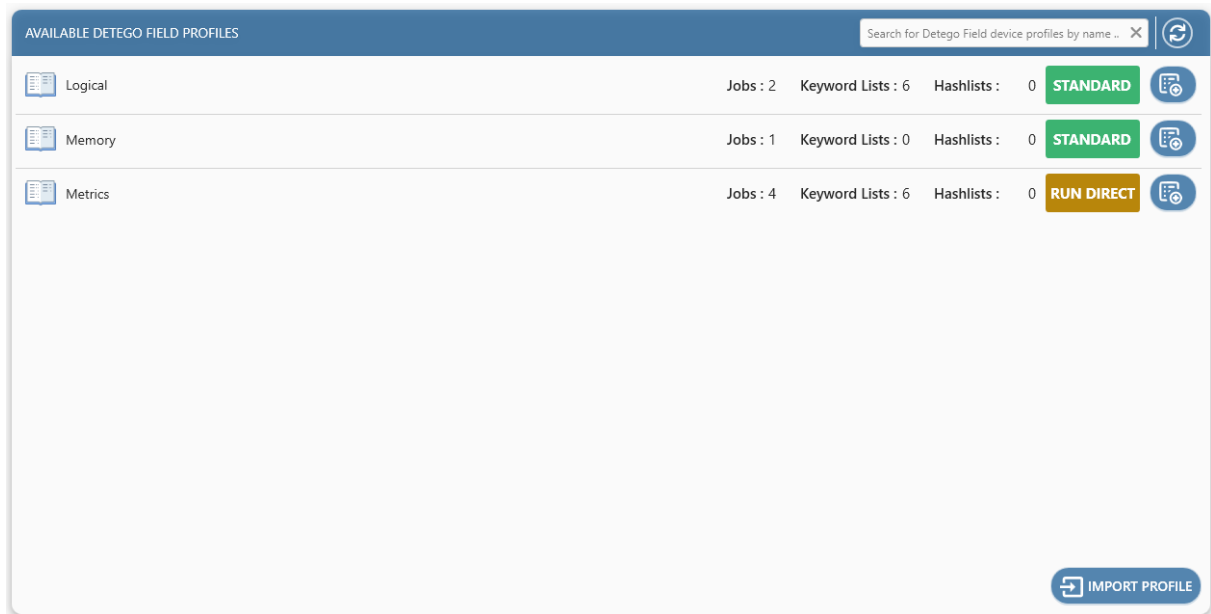


- Once the Harvest window above has opened (it will vary depending on the profiles created on the device), tick the checkboxes on the profiles you wish to import and then select HARVEST.

DETEGO FIELD PROFILE MANAGEMENT

Once you have harvested some profiles, you can return to the 'Field Profiles' tab on the Configuration window. You will see your Field Profiles listed in the window:

Figure 94

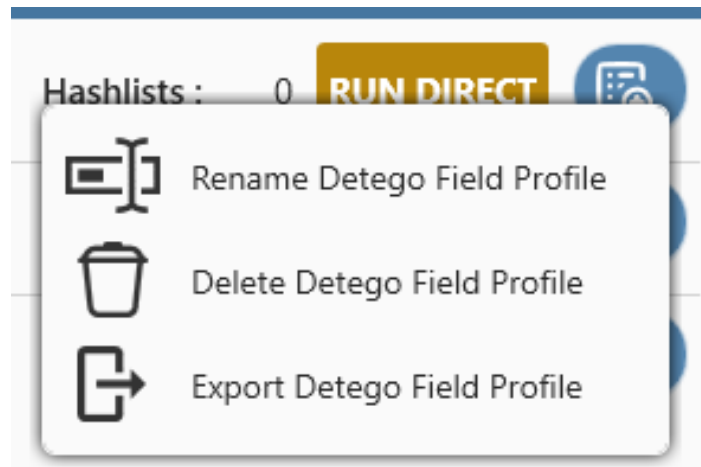


- Selecting the 'RUN DIRECT' button will switch between RUN DIRECT and STANDARD options.
- These establish whether the profile can be run directly from the root Field folder or as standard Field jobs within CONFIG.

The **MANAGE** Button

- Select the "MANAGE" button on the right side of the Field Profile you wish to manage. This will bring up a list of options available for the Field Profile. These include:
 - 'Rename Field Profile' – Allows renaming of the Field Profile
 - 'Delete Field Profile' – Deletes the Field Profile
 - 'Export Field Profile' – Exports the Field Profile

Figure 95



RENAME DETEGO FIELD PROFILE

- Select the 'Rename Field Profile' option from the list to rename.
- Type in what you wish to rename your field profile and select OK.

Figure 96

DELETE DETEGO FIELD PROFILE

- Select the 'Delete Field Profile' option from the list to delete.
- Select YES if you wish to delete the Field Profile or NO if you wish to cancel the operation.

Figure 97

EXPORT DETEGO FIELD PROFILE

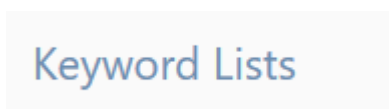
- Select the 'Export Field Profile' option from the list to export.
- Browse to a location to save the 'Detego Field Profiles' (.dfp) and click Save.
- To import a Field Profile, select the 'IMPORT PROFILE' button in the bottom right corner of the Field Profiles window. Browse for the Detego Field Profile (.dfp) file and select Open to import the Field Profile.

3.8. CONFIGURING KEYWORD/REGEX LISTS

Keyword matching is an examination technique for identifying relevant evidence by searching the content acquired from a digital device using a pre-determined list of keywords imported into the Detego Platform. Matches can be made even if the word or phrase is in unallocated space or deleted files.

Note: Before creating a keyword list, a text (.txt) file containing the line-separated keywords should be created and ready for import.

Figure 98



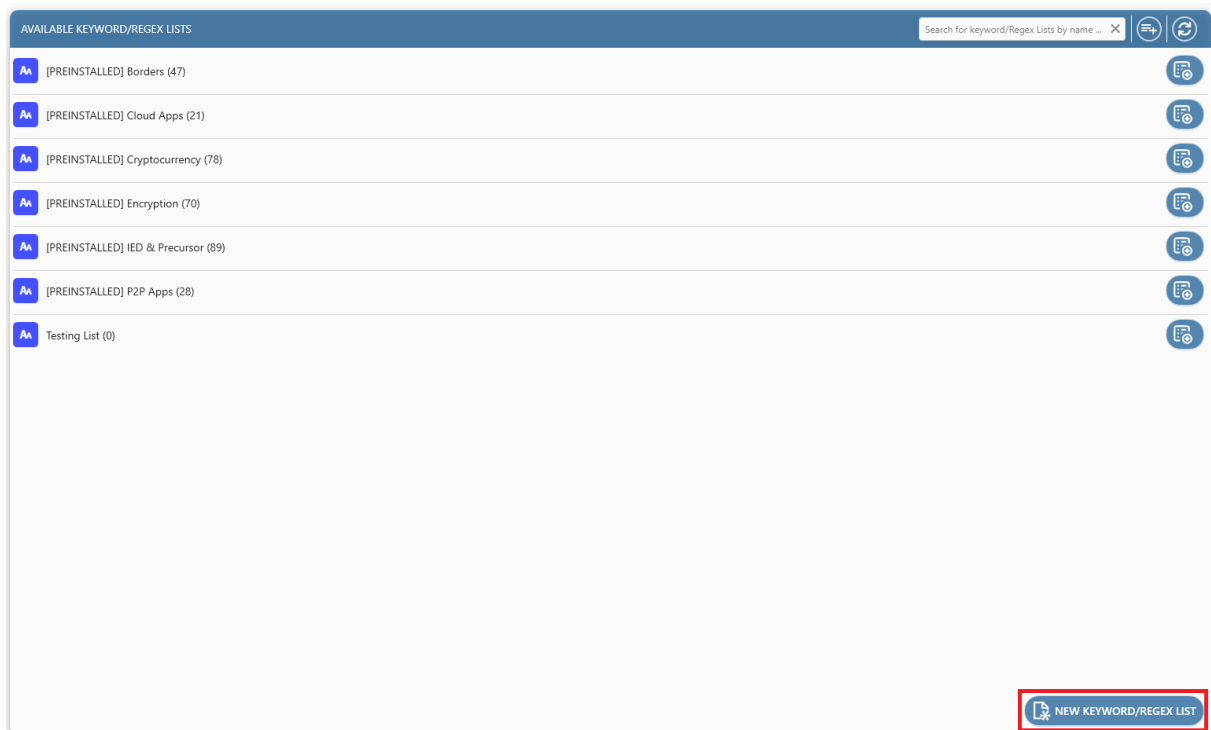
PLEASE NOTE! There is a separate guide on correctly writing the syntax for a Regex list, as that is more complex.

CREATING A KEYWORD / REGEX LIST

To create a Keyword / Regex list, please follow the below steps:

- Select the 'NEW KEYWORD/REGEX LIST' button in the bottom right corner.

Figure 99



- Input the 'Name' for your Keyword/Regex List.
- Select either 'Standard' or 'Regex' options to choose whether it's a regular keyword list or Regex list.
- Select CREATE in order to create the Keyword List.

Figure 100

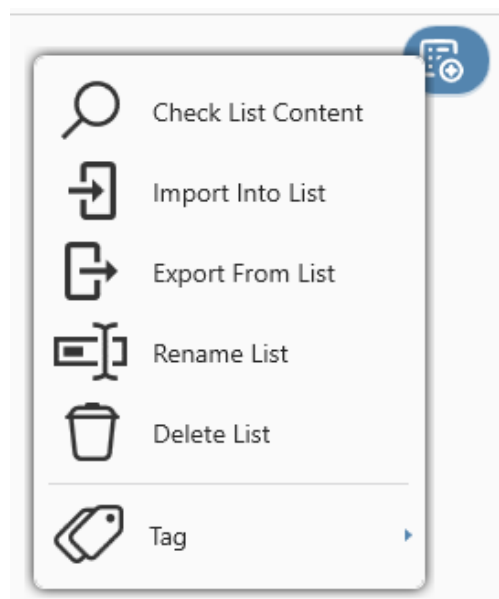
A screenshot of a form titled 'Create New keyword/Regex List'. The form has a subtitle 'Please enter details for this keyword/Regex List:'. Below the subtitle is a text input field labeled 'keyword/Regex List Name:'. Underneath the input field are two radio buttons: 'Standard' (which is selected) and 'Regex'. To the right of the 'Regex' radio button is an information icon. At the bottom of the form, there is a red error message that says 'Please enter a name for this keyword/regex list'. To the right of the error message are two buttons: 'CREATE' and 'CANCEL'.

MANAGING A KEYWORD / REGEX LIST

Selecting the button on the right side of the keyword list presents you with various options to manage your keyword lists. These are the following:

- Check List Content
- Import Into List
- Export From List
- Rename List
- Delete List
- Tag

Figure 101

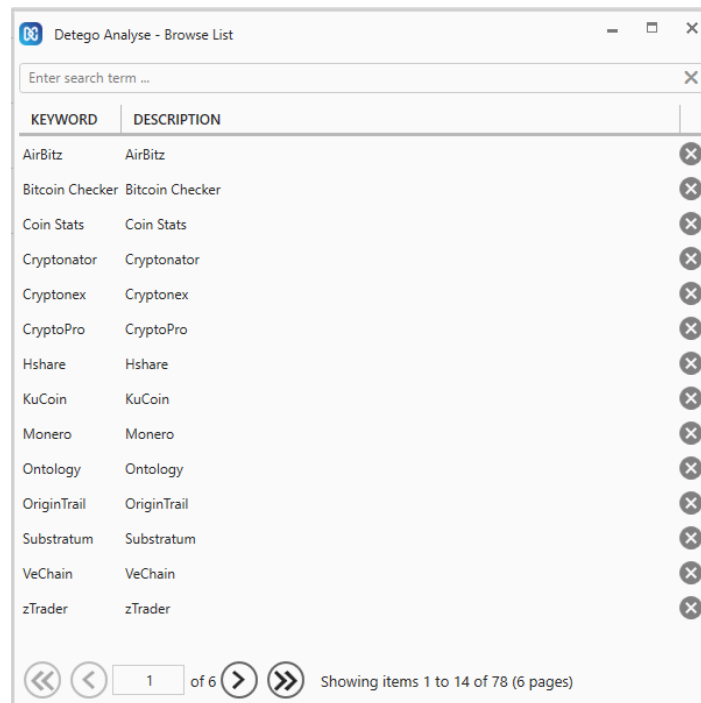


CHECK LIST CONTENT

This window displays a list of all the imported keywords. From here, the investigator can search for a particular keyword or check any/all keywords.

- Select the 'Check List Content' from the list of options.
- If you are searching for a particular Keyword/Regex, type it into the input box at the top of the 'Browse List' screen.

Figure 102



- You can remove an individual keyword by selecting the '(X)' icon on the right of the keyword.
- Select the navigation icons at the bottom of the window to navigate the pages.

IMPORT INTO LIST

You can either import keywords from a file, i.e., a line separated .txt file, or 'Manual Input...' whereby the keywords are manually typed. Separate each keyword by placing it on a new line.

There is also support for "Wildcards". Wildcards are special characters that represent different functions within a word/text. This includes the characters below within the square brackets:

[.] – Matches any single character except the new line character (\n), e.g., "ra.n" will match "rain", "rael", and "raul".

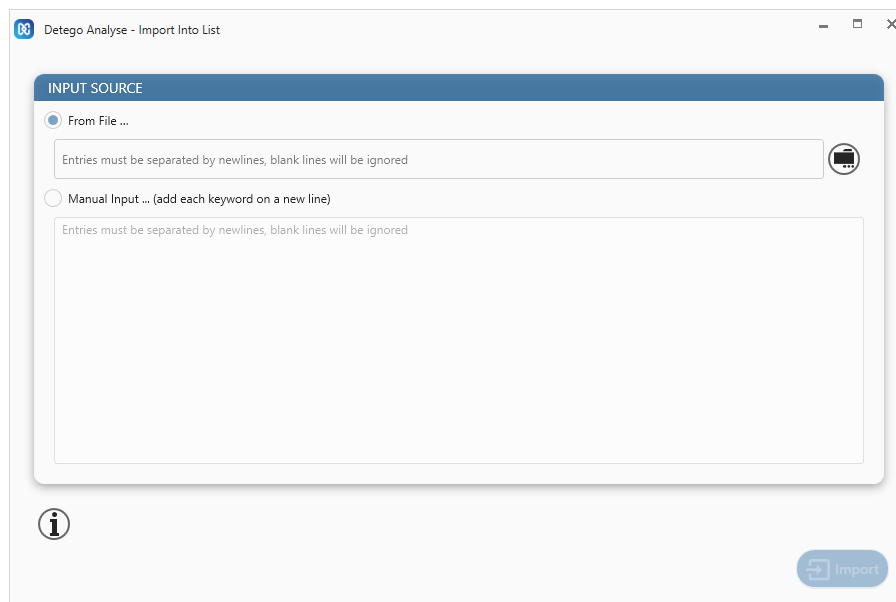
[?] – Matches the last element 0 or one time. e.g., "ra?n" will match "ran" and "rain".

[*] – Works similar to the [?] except that it matches 0 or more instances of the preceding character.

- Select the 'Import Into List' option from the list.
- Select one of the radio buttons to choose whether to import 'From File...' or 'Manual Input...'.

- From file allows you to choose a file to import from, whereas Manual Import allows you to type the keywords manually.
- If the import is successful, a message will display in the bottom left corner showing the number of keywords imported (any duplications are ignored).

Figure 103



If you are unsure about the Lucene, you can select the (i) button in the Import Into List window. This will provide you more information on how to structure your keywords.

EXPORT FROM LIST

This function exports a keyword list into a line-separated .txt file for use on another system or for storage.

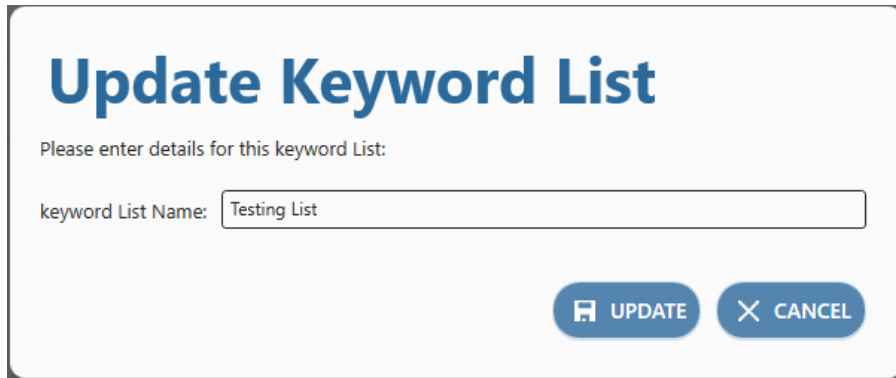
- Select the 'Export From List' option in the list.
- Name the list and save it in an appropriate location in the File Explorer window.
- Once saved, the user is returned to the 'AVAILABLE KEYWORD LISTS' screen. The exported item can then be viewed as a list of line-separated keywords in a text (.txt) file in Notepad.

RENAME LIST

From here, you can change the name of the keyword/regex list.

- Select the 'Rename List' option from the list.
- Enter the name you wish to use for the keyword list and select UPDATE.

Figure 104



Update Keyword List

Please enter details for this keyword List:

keyword List Name:

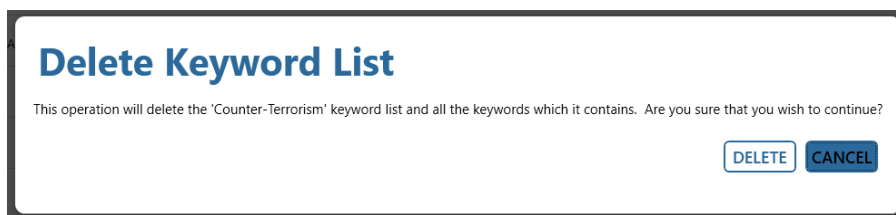
 UPDATE  CANCEL

DELETE LIST

From here, you can remove keyword/regex lists from Detego Analyse.

- Select the 'Delete List' option from the list.
- Confirm the deletion when the prompt appears by selecting the 'DELETE' button or 'CANCEL' to cancel the operation.

Figure 105



Delete Keyword List

This operation will delete the 'Counter-Terrorism' keyword list and all the keywords which it contains. Are you sure that you wish to continue?

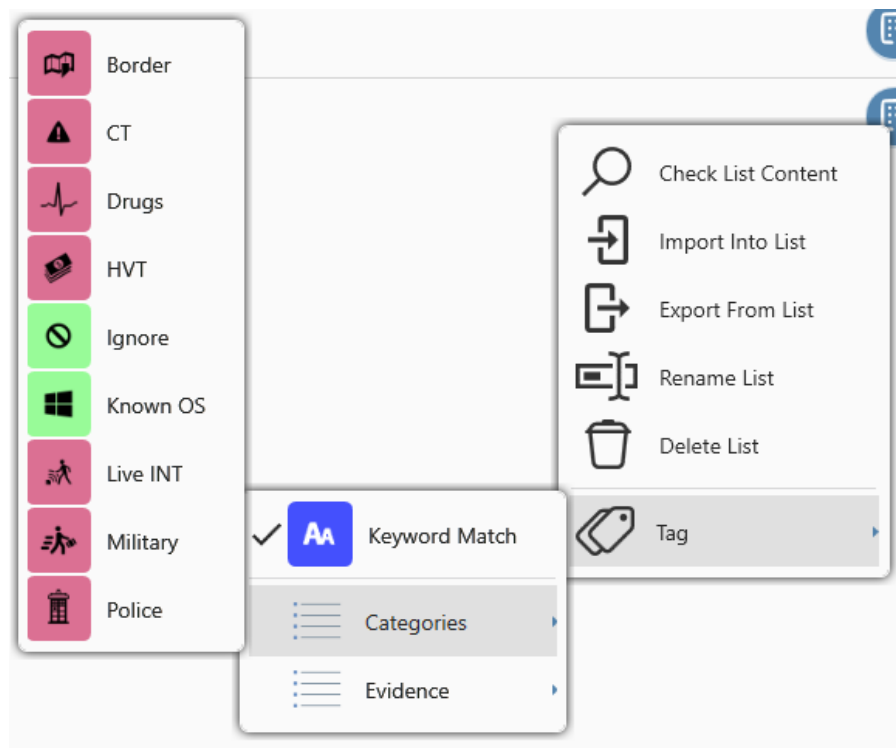
DELETE CANCEL

TAG

This allows you to specify the tag applied to items that match keywords from your lists.

- Select the 'Tag' option from the list and then select the tag you would like to apply to the keywords matched within the list automatically.

Figure 106



3.9. CONFIGURING STORAGE VOLUMES

Detego Storage is the space where all extracted cases are stored. Users can register and deregister various disk volumes from this module, including physically connected drives. Before starting extractions, you will need to add a storage volume.

Figure 107

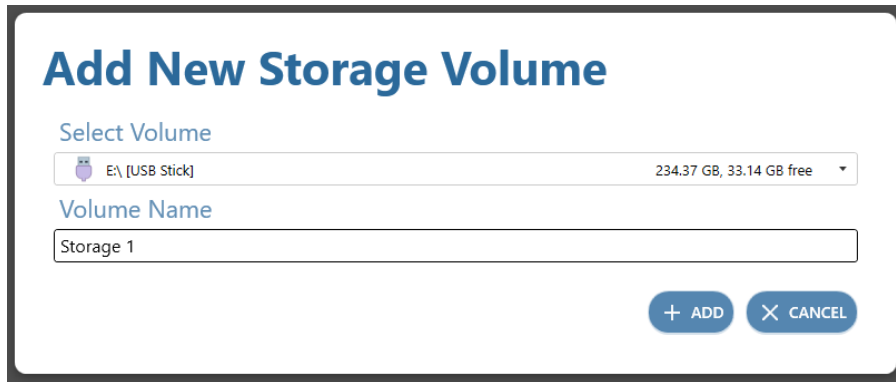
Storage

ADDING A STORAGE VOLUME

To add a Storage Volume, follow the below steps:

- Select the 'ADD' button in the bottom right corner.
- Select the storage volume you wish to add from the new 'Add New Storage Volume' window and select the '+ ADD' button.
- Once added, the storage volume is visible on the Storage Volumes screen.

Figure 108

A dialog box titled "Add New Storage Volume" in blue. It has a section "Select Volume" with a dropdown menu showing "E:\ [USB Stick]" and "234.37 GB, 33.14 GB free". Below this is a "Volume Name" section with a text input field containing "Storage 1". At the bottom right are two buttons: "+ ADD" and "X CANCEL".

Add New Storage Volume

Select Volume

E:\ [USB Stick] 234.37 GB, 33.14 GB free

Volume Name

Storage 1

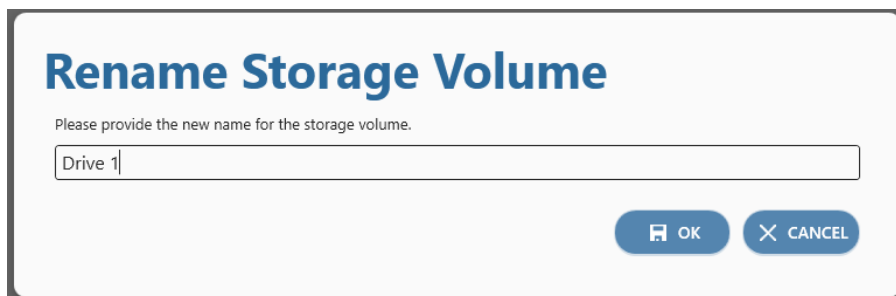
+ ADD X CANCEL

NOTE! Storage Volumes MUST be a minimum of 100GB and formatted as NTFS. We highly recommend using a large SSD (Solid State Drive) rather than HDD (Hard Disk Drive) due to the significantly slower performance, though HDDs are supported as Storage Volumes.

RENAMING A STORAGE VOLUME

To rename a Storage Volume, select the 'RENAME' button on the Storage Volume from the list and input your new Storage Volume name.

Figure 109

A dialog box titled "Rename Storage Volume" in blue. It has a text input field with the placeholder "Please provide the new name for the storage volume." and the text "Drive 1" entered. At the bottom right are two buttons: "OK" and "X CANCEL".

Rename Storage Volume

Please provide the new name for the storage volume.

Drive 1

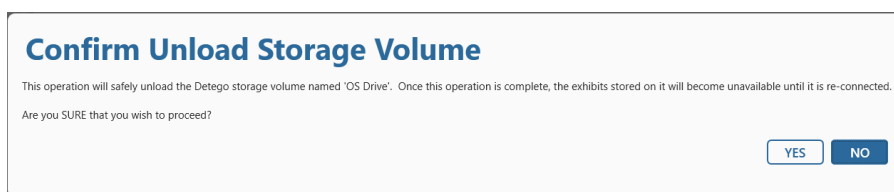
OK X CANCEL

UNLOADING A STORAGE VOLUME

Unloading Storage Volumes is a feature for safely unloading a storage volume from Detego. It should be used to prevent data loss when physically disconnecting the volumes from a running Detego instance. The Unload function also creates a database backup of the cases/exhibits stored on the volume.

To unload a Storage Volume, select the 'UNLOAD' button on the Storage Volume from the list and select YES if you wish to unload the volume or NO if you wish to cancel the operation.

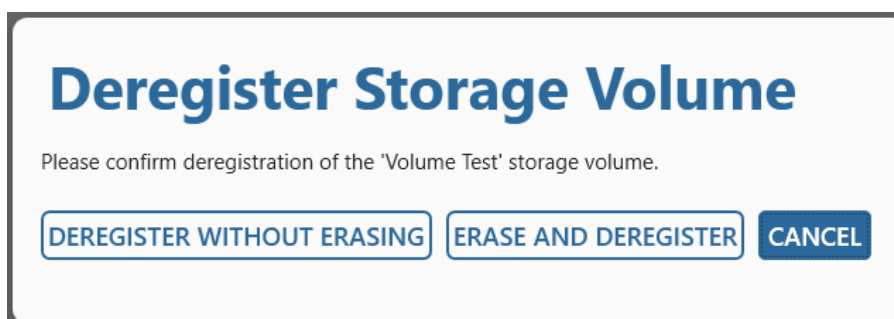
Figure 110



DEREGISTERING A STORAGE VOLUME

Deregistering a Storage volume is for putting a volume in an unregistered state. The Detego Platform will no longer load the case or exhibit content. Only use this feature if the data on the volume is no longer required. It can only be performed on an 'Unloaded' storage volume.

Figure 111



DEREGISTER WITHOUT ERASING

This will Deregister the Storage Volume without completely erasing it. Once you have disconnected the storage volume, you can reconnect it later, and Detego will reconcile it (if the external drive is reinserted, it will automatically re-register it). The below images are the messages that appear when Deregistering without erasing and then Reconnecting (Left to right).

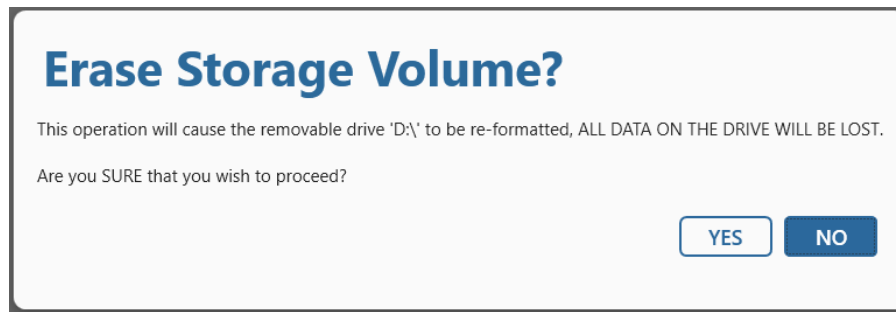
Figure 112



ERASE AND DEREGISTER

This will Deregister the Storage Volume and erase all data so it will not be recoverable. Once deregistered as a Storage Volume, it will be registered as a Non-Evidence Volume.

Figure 113



WARNING! This will erase all data on the storage volume and won't be recoverable, so make sure you DO NOT need the data anymore and move any exhibits to another storage volume to prevent any data loss.

BACKING UP EXHIBITS

We strongly advise backing up your exhibits regularly to prevent loss of data. The best possible method of backing up your exhibits is by following the below steps:

- Select the exhibit you wish to back up and select the 'Export' button from the CASE MANAGEMENT window.
- Select the 'Detego Package Export' job from the available export options.
Choose a location to save the export.

This will create a Detego Export Package (.dep) to be imported into Detego Analyse when needed. This is the main backup option; the next steps should only be done if these previous steps have been followed first.

You can also insert an external Storage Device and add it as a Storage Volume. Once added, move the exhibits you wish to backup onto the external Storage Volume. Once you have moved all the exhibits, navigate to Configuration, then 'Storage'. Select the 'UNLOAD' button on your "Backup" Storage Volume, and then once successful, you can remove the Storage Volume.

3.10. CONFIGURING NON-EVIDENCE VOLUMES

Detego Non-Evidence Volumes are similar to Storage Volumes; however, they will not be treated as 'Target' devices when detected. They will be ignored until deregistered.

Figure 114

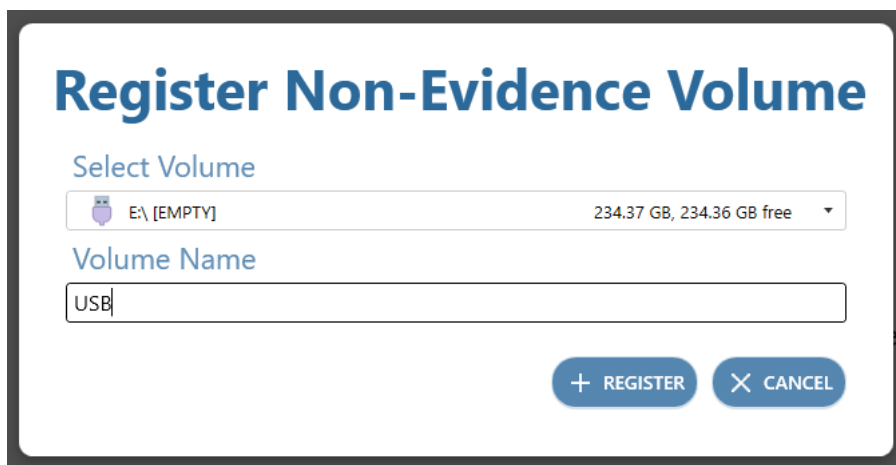
Non-Evidence

ADDING A NON-EVIDENCE VOLUME

To add a Non-Evidence Volume, follow the below steps:

- Select the '+ ADD' button in the bottom right corner of the screen.
- Select the volume from the dropdown.
- Input your Volume Name.
- Select 'REGISTER'

Figure 115



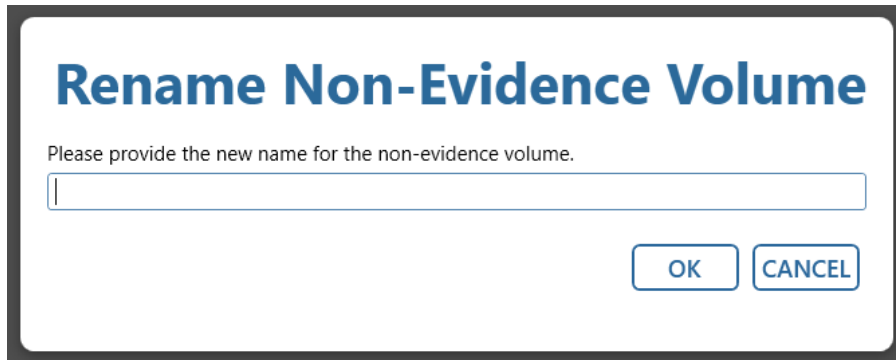
The dialog box titled "Register Non-Evidence Volume" contains two main sections. The first section, "Select Volume", features a dropdown menu with a purple USB icon, the text "E:\ [EMPTY]", and a status indicator "234.37 GB, 234.36 GB free" with a downward arrow. The second section, "Volume Name", has a text input field containing "USB". At the bottom right, there are two buttons: a blue button with a plus icon and the text "REGISTER", and a grey button with an 'X' icon and the text "CANCEL".

RENAMING A NON-EVIDENCE VOLUME

To rename a Non-Evidence Volume, follow the below steps:

- Select the 'RENAME' button on the Non-Evidence Volume you wish to rename.
- Input the new volume name and select OK to save the changes.

Figure 116

A dialog box titled "Rename Non-Evidence Volume" in bold blue text. Below the title, it says "Please provide the new name for the non-evidence volume." followed by a text input field. At the bottom right, there are two buttons: "OK" and "CANCEL".

Rename Non-Evidence Volume

Please provide the new name for the non-evidence volume.

OK CANCEL

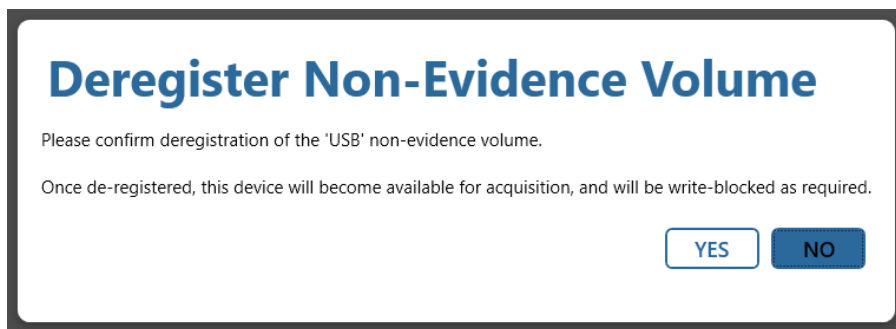
DEREGISTERING A NON-EVIDENCE VOLUME

Deregistering a Non-Evidence Volume will mark it as an evidence volume again and be detected for extraction.

To deregister a Non-Evidence Volume, follow the below steps:

- Select the 'DEREGISTER' button on the Non-Evidence Volume you wish to deregister as nonevidence.
- Select YES if you wish to deregister or NO if you wish to cancel the operation.

Figure 117

A dialog box titled "Deregister Non-Evidence Volume" in bold blue text. Below the title, it says "Please confirm deregistration of the 'USB' non-evidence volume." followed by "Once de-registered, this device will become available for acquisition, and will be write-blocked as required." At the bottom right, there are two buttons: "YES" and "NO".

Deregister Non-Evidence Volume

Please confirm deregistration of the 'USB' non-evidence volume.

Once de-registered, this device will become available for acquisition, and will be write-blocked as required.

YES NO

3.11. CONFIGURING REMOTE ACQUISITION SETTINGS

The Remote Acquisition settings allow you to adjust parameters of your Remote Acquisition jobs.

Figure 118

Remote Acquisition

- Selecting the browse icon on the “Uploads Folder” will let you select a location to upload to.
- You can adjust the Logical Acquisition Filestore Limit using the other setting.

Figure 119

3.12. CONFIGURING EXTRACTION OPTIONS

Extraction Options allows extraction parameters to be setup for when running imaging jobs.

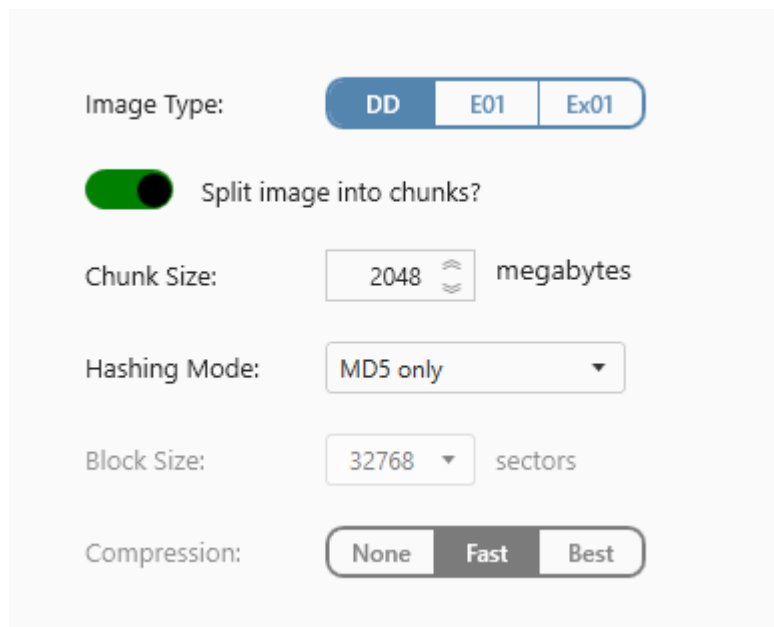
Figure 120

Extraction Options

The Extraction Options are included below:

- **Image Type** - Allows you to select the type of Image file. (DD, E01, Ex01)
- **Split Image into chunks** - Allows you to select whether images are split into chunks, On/Off. (Only available for DD)
- **Chunk Size** - Allows you to determine the Chunk Size if above setting is enabled.
- **Hashing Mode** - Allows you to select what hashing method is used. (MD5 only, MD5 and SHA1, MD5 and SHA256)
- **Block Size** - Allows you to determine the block size in sectors. (Not available for DD)
- **Compression** - Allows you to select a compression type. (Not available for DD)
 - **None** - No compression
 - **Fast** - Fast compression
 - **Best** - Best compression

Figure 121



The image shows a configuration window with the following settings:

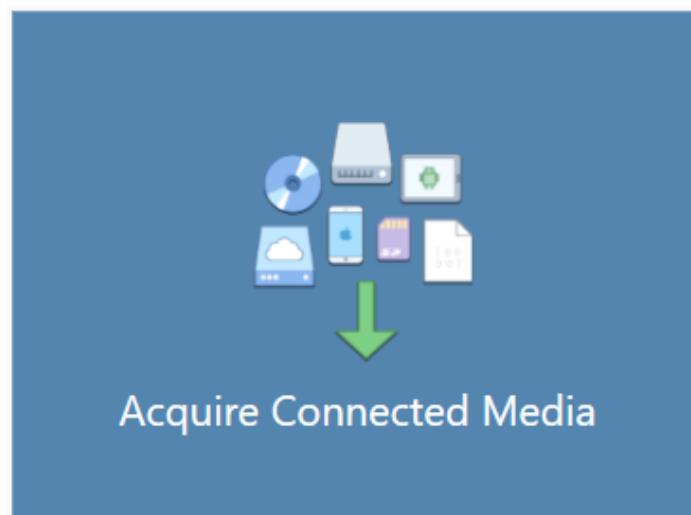
- Image Type:** A group box containing three buttons: **DD** (selected), **E01**, and **Ex01**.
- Split image into chunks?** A toggle switch that is currently turned on (green).
- Chunk Size:** A text input field containing **2048**, followed by a unit selector showing **megabytes**.
- Hashing Mode:** A dropdown menu currently set to **MD5 only**.
- Block Size:** A text input field containing **32768**, followed by a unit selector showing **sectors**.
- Compression:** A group box containing three buttons: **None**, **Fast** (selected), and **Best**.

Whilst these options change the defaults, you can still manually override when setting up an extraction if required.

4. ACQUIRE CONNECTED MEDIA

The 'Acquire Connected Media' tile on the Detego Home Screen is where you will be able to choose your extraction/acquisition method.

Figure 122

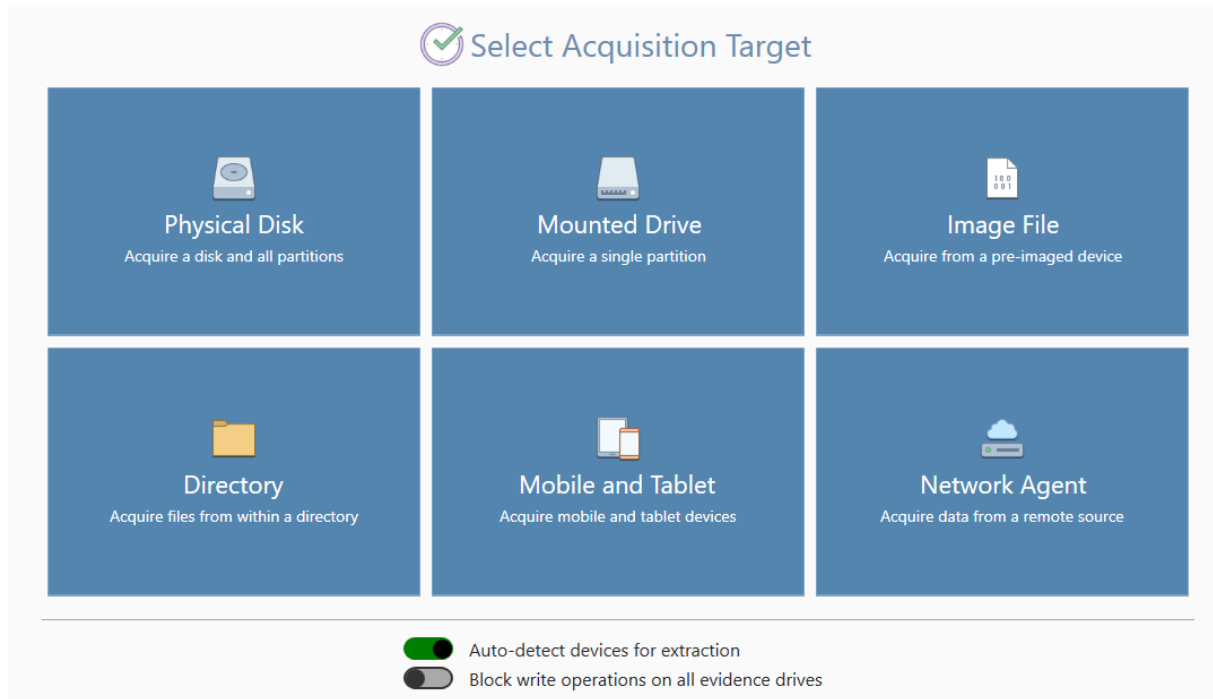


Once you have selected the 'Acquire Connected Media' tile, it will bring you to the 'Acquire Media' screen.

Some of the target devices that you can forensically exploit using Media Acquisition include the following:

- USB Storage Drives
- SD and Micro-SD Cards
- IDE and SATA Drives (SSDs and HDDs)
- M.2 NVME SSDs
- Mobile Phones and Tablets

Figure 123



NOTE! Accessibility to extraction types may vary depending on your license. The Mobile and Tablet is only available if you are licensed and have access to our integrated Mobile Forensic software.

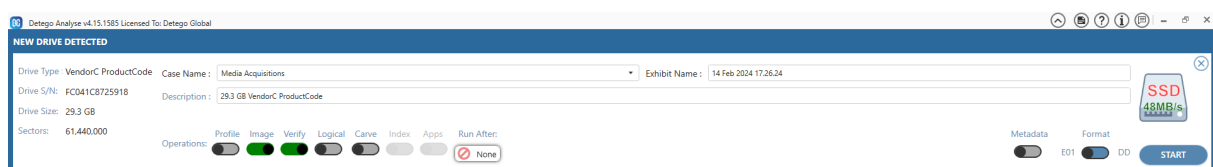
The Network Agent tile requires additional procedures to setup correctly. If you do not have access and would like more information, please contact marketing@detegoglobal.com.

4.1. AUTO-DETECT

The Auto-Detect option enables the automatic dropdown when a device is connected to the Detego Analyse machine. If toggled on, the dropdown will display when a device is connected and you can acquire data from the device using the dropdown for a basic acquisition.

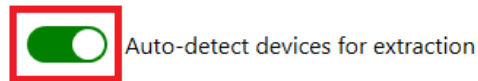
This does not apply to Detego Field Devices, Storage Volumes, Detego Ballistic Collectors or Non-Evidence Volumes.

Figure 124



- To enable/disable the auto-detect feature, select the 'Auto-detect devices for extraction' toggle button from within the 'Acquire Connected Media' tile.

Figure 125



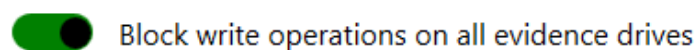
4.2. WRITE BLOCKING

Detego Analyse allows the operator to write-block the USB device at the logical disk level on the analytical machine to enable a forensic read-only capability. By default, it is switched off.

CAUTION! Please be aware that we use a propriety Windows filter driver that is well-supported and maintained; however, it should be noted that it blocks at the logical disk level, not physical. If you need write-blocking at the physical level, you **MUST** use hardware writeblockers.

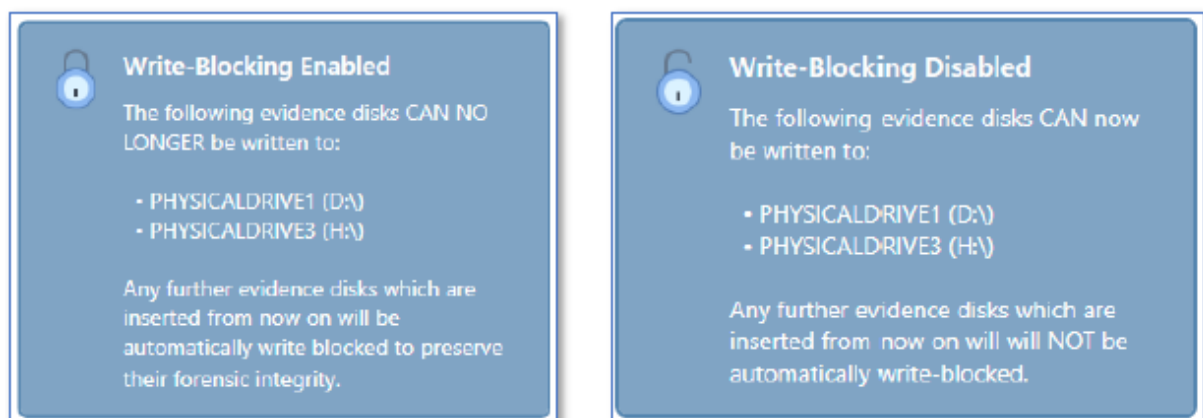
- To enable/disable the write-blocking feature, select the 'Block write operations on all evidence drives' toggle button from within the 'Acquire Connected Media' tile.

Figure 126



Below are the messages that appear when Write-blocking is enabled/disabled.

Figure 127



NOTE! The write-blocking functionality applies to all devices connected to Detego Analyse while the program is running, except for:

- Detego Field Devices
- Storage Volumes
- Detego Ballistic Collectors
- Non-Evidence Volumes

Please be aware that Write-blocking is active only while the client logs in. Devices become writable again when the Detego client is not running (even if the server is).

To revoke the USB write-blocking, toggle the switch to the 'Off' (greyed) position. It is also advisable to restart the device where possible.

4.3. DETEGO ANALYSE DISK INSPECTOR

Detego Analyse Disk Inspector allows you to browse the file tree before extracting any files. It also allows you to select which files you want to extract. Files can be previewed before extraction into an automatically created exhibit (stored within a case named 'Disk Inspector').

To use Detego Analyse Disk Inspector, follow the steps below:

- Insert the target media into your Detego Analyse machine. (The 'Auto-Detect' dropdown is not relevant for Disk Inspector. Please close the dropdown if it shows up when inserting media.)
- Select the 'Acquire Connected Media' tool tile from the home screen.
- Select the relevant 'Physical Disk' or 'Image File' tiles from the Media Acquisition screen. These are the only two tiles where Disk Inspector is available.

Figure 128

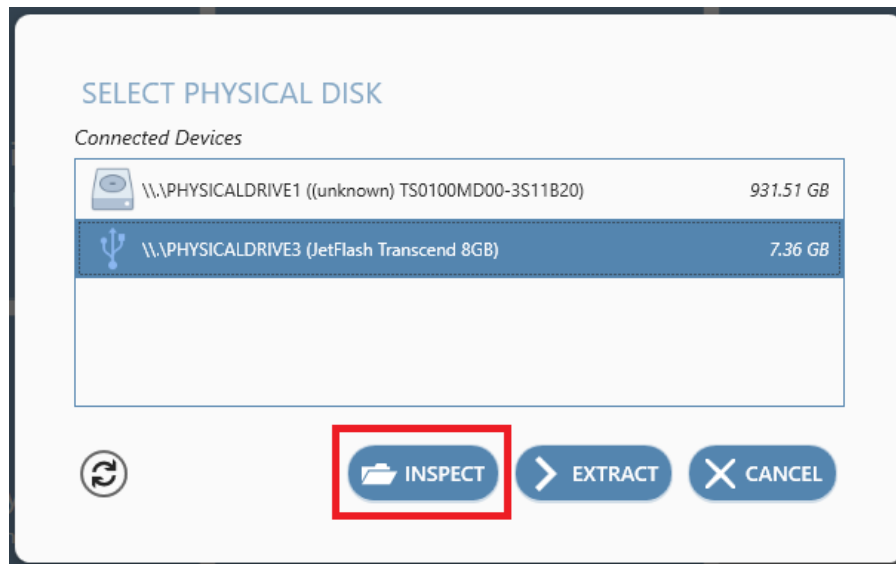
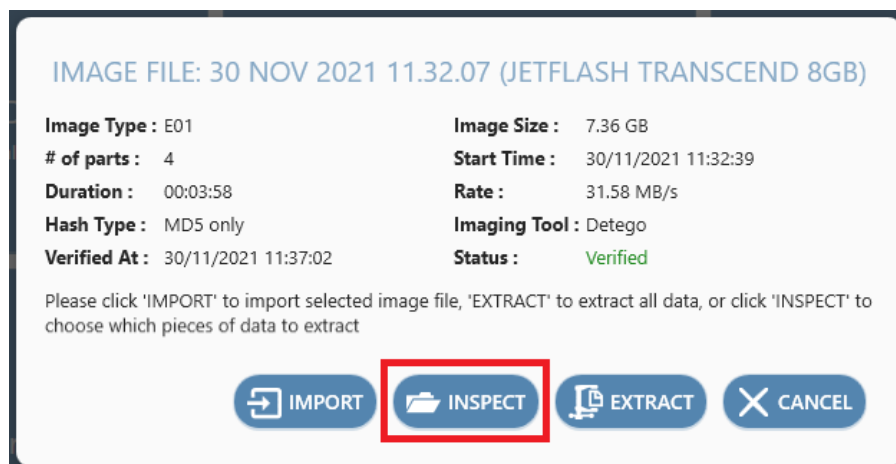


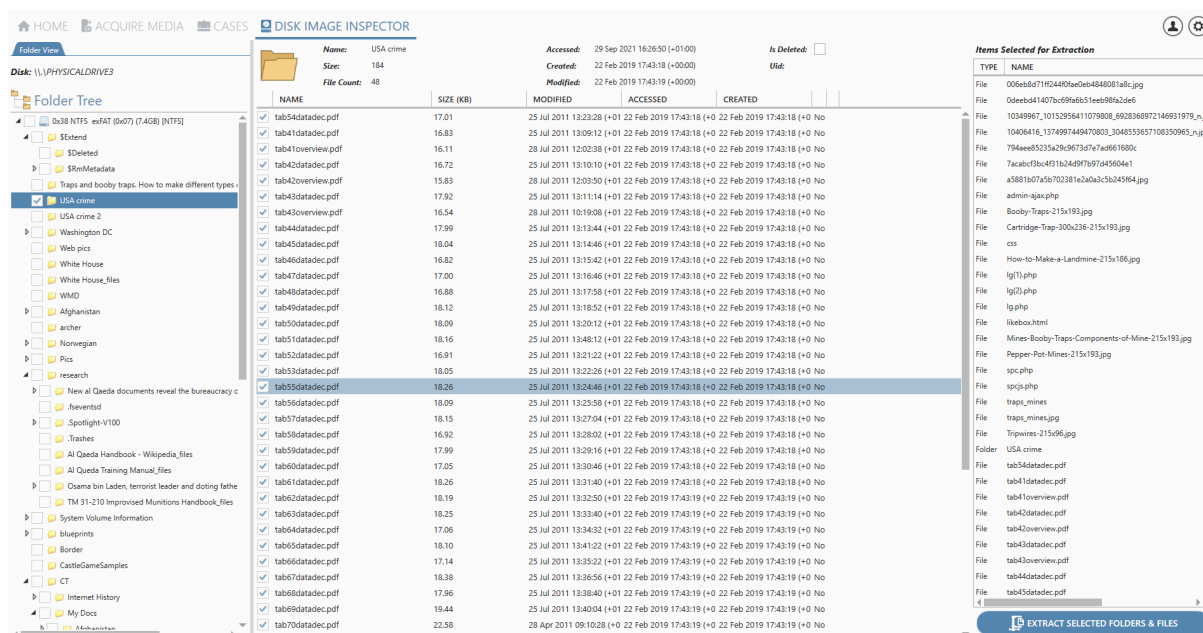
Figure 129



- Select the target device/file and click INSPECT.
- The file tree will load and then display the following:
 - The left panel displays the folder tree of the target. Folders and subfolders can be collapsed and expanded where applicable.
 - The central panel displays files within the currently selected folder.
 - The right panel displays the files and folders selected to be extracted and the details

for the items selected. Ticking items in the other two panels will add them to this list.

Figure 130



- If Drive Image files are being inspected, deleted items will appear marked and can be carved.
- Files can be previewed in the omniviewer by right-clicking and selecting 'Extract File Preview'.
- To extract all selected items (displayed in the right panel), click the extract button in the bottom right corner, and the job will run. Files are placed in an automatically created case exhibit.

BITLOCKER PARTITIONS

Detego Analyse Disk Inspector supports inspecting Images and Physical Drives with BitLocker partitions. If a BitLocker partition is detected in the forensic image or physical drive which is being inspected, a prompt will display requiring the BitLocker password or recovery key for the partition.

Figure 131



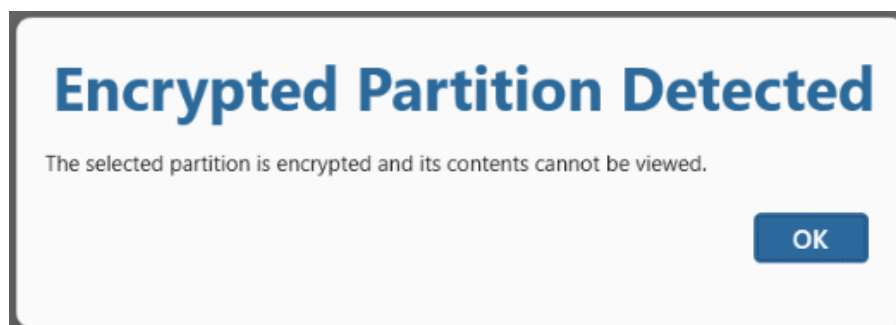
The 'CHECK PASSWORD' button is used to verify if the supplied password or recovery key is able to decrypt the BitLocker partition.

Once a valid BitLocker password or recovery key is supplied, the BitLocker partition is decrypted and can be inspected normally.

You can select the 'SKIP' button in order to skip the decryption process. The skipped BitLocker partition will be listed in the Folder Tree but will not be available for inspection.

The below prompt will be displayed when selecting an encrypted partition.

Figure 132



4.4. PHYSICAL DISK

PHYSICAL DISK - DROPDOWN METHOD

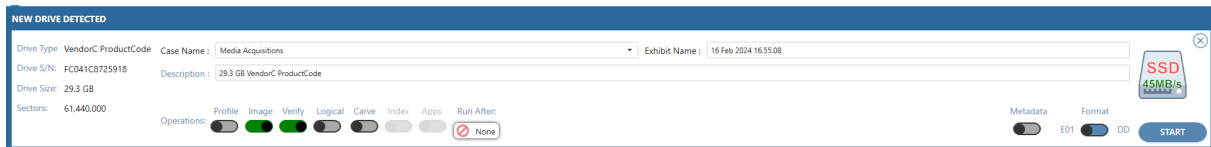
This extraction method from a Physical Disk allows a quick setup process and requires less technical knowledge. The 'Auto-detect' option must be enabled for the dropdown to appear.

To acquire data from a Physical Disk, conduct the following steps:

- Insert your target media into your Detego Analyse machine.

- At the top of the screen, Detego's Auto-Detect dropdown will display details of the device you inserted into the machine.

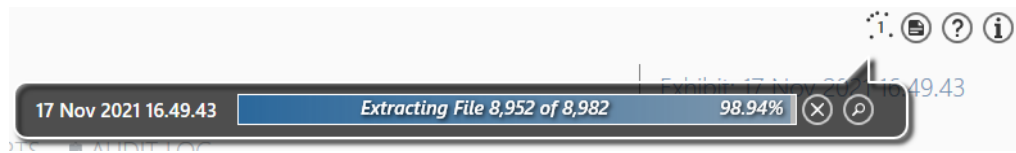
Figure 133



- From here, you can edit the 'Case Name', 'Exhibit Name' and 'Description' if you wish. These will auto-populate with some details depending on the device and date. You can also change this later within the Case Management module.
- Use the toggle buttons to add certain jobs for the extraction. Below is a quick overview of the settings available:
 - **'Profile'** – Acquires the System Information of the target device if applicable.
 - **'Image'** – Acquires the bit-for-bit image of the target device. This is defaulted to E01 but can be adjusted using the 'Format' option on the right side of the dropdown.
 - **'Verify'** – Verifies the image. (Must have 'Image' toggled on).
 - **'Logical'** – Acquires the logical files from the target device.
 - **'Carve'** – Performs a file carving job to uncover deleted files.
 - **'Index'** – Runs the 'Text Index' job. (Requires Logical or Carve to be selected).
 - **'Apps'** – Runs the 'App Parsing' job. (Requires Logical or Carve to be selected).
 - **'Run After'** - Allows you to select and run a pre-saved Job Queue.
 - **'Metadata'** - You can edit the exhibit metadata before starting the acquisition.
 - **'Format'** – Allows you to change the imaging format from the default E01 Imaging to DD. (Must have 'Image' toggled on).
- When you are happy with your settings, select START.

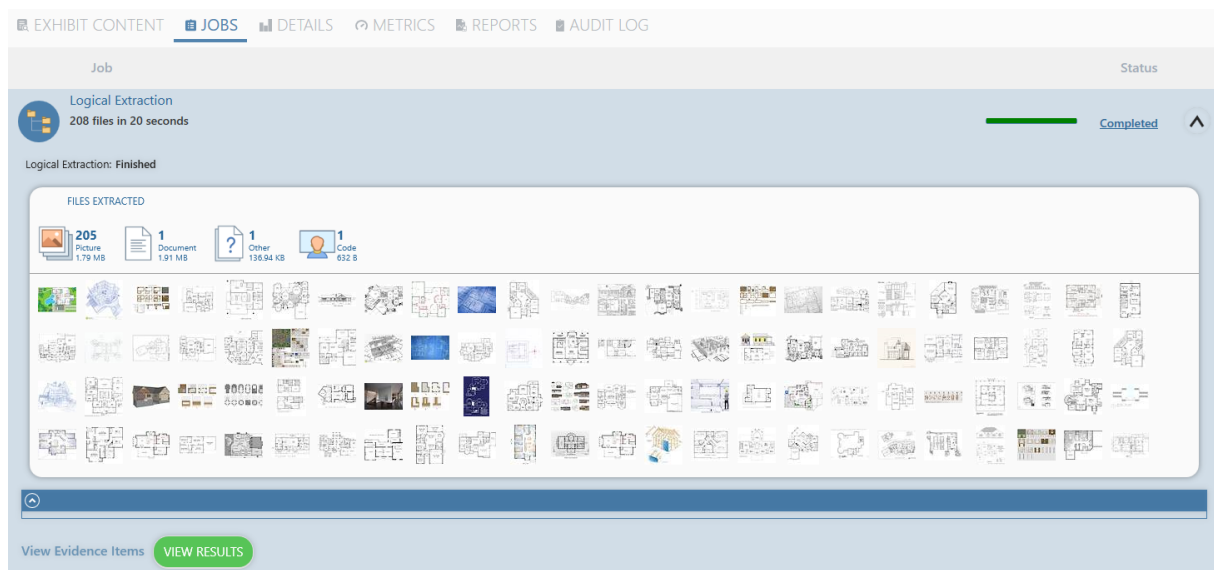
- A progress bar will display at the top of the screen, which shows the current job that is being run and the proportion that has been completed.

Figure 134



- The data extracted from the acquisition will be visible within the 'Jobs' tab of the Exhibit within the 'Analyse and Manage' module.

Figure 135



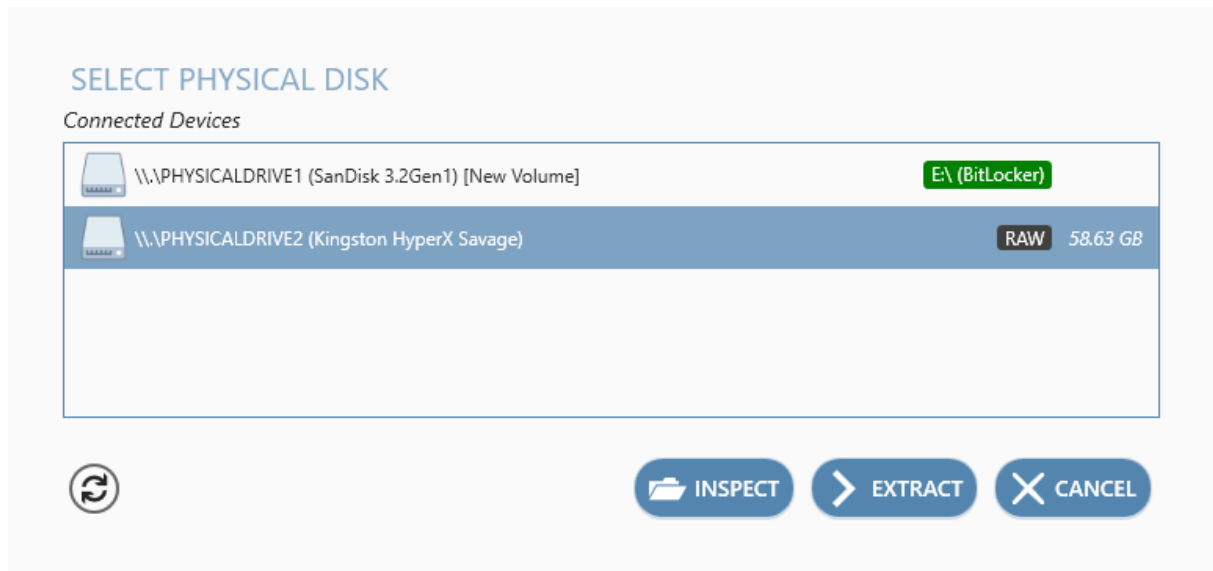
PHYSICAL DISK - ADVANCED METHOD

The advanced method for acquiring data from a Physical Disk allows you to make a series of fine selections to determine the exact data you wish to acquire and the follow-up analytics you'd like to conduct.

If the 'Auto-detect' dropdown has appeared, close it.

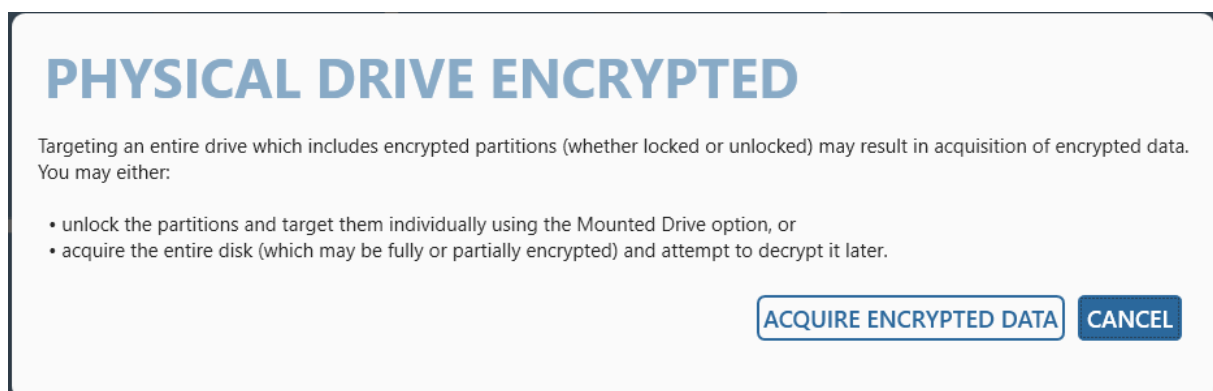
- Select the 'Acquire Connected Media' module from the home screen and select the 'Physical Disk' tile.
- Select the target drive from the list of connected devices and then select 'EXTRACT'.

Figure 136



- If the drive is encrypted, selecting the EXTRACT button will display the below message. If the drive is not encrypted, selecting EXTRACT will skip this part and take you straight to the Configure Acquisition window.
- You can either:
 - Select CANCEL, then unlock the partitions and target them individually using the Mounted Drive option.
 - Select ACQUIRE ENCRYPTED DATA to acquire the entire disk (which may be fully or partially encrypted) and attempt to decrypt it later.

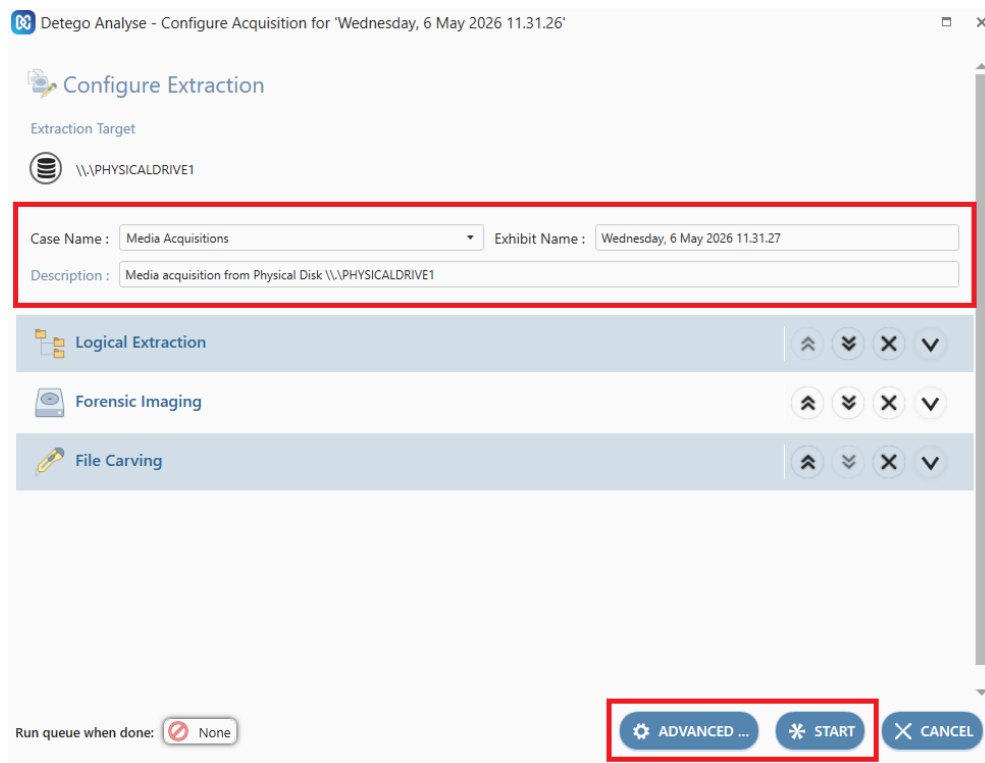
Figure 137



- After selecting EXTRACT for non-encrypted drives or ACQUIRE ENCRYPTED DATA for encrypted drives, you will see the Configure Acquisition window.

- From here, you can adjust the Case Name, Exhibit Name, and description of the exhibit.
 - By default, the Physical Disk Extraction will run the Logical Extraction, Forensic Imaging and then File Carving jobs; however, you can configure this to your specification and select START, or you can select the ADVANCED to change the job queue in depth.

Figure 138



- Selecting each of the jobs (or selecting the dropdown arrow (v) on the right side of the jobs) will open up some more advanced options for the jobs.

NOTE! For more information on Jobs; please navigate to the 'Analytics' portion of the 'Analyse and Manage' section within this guide.

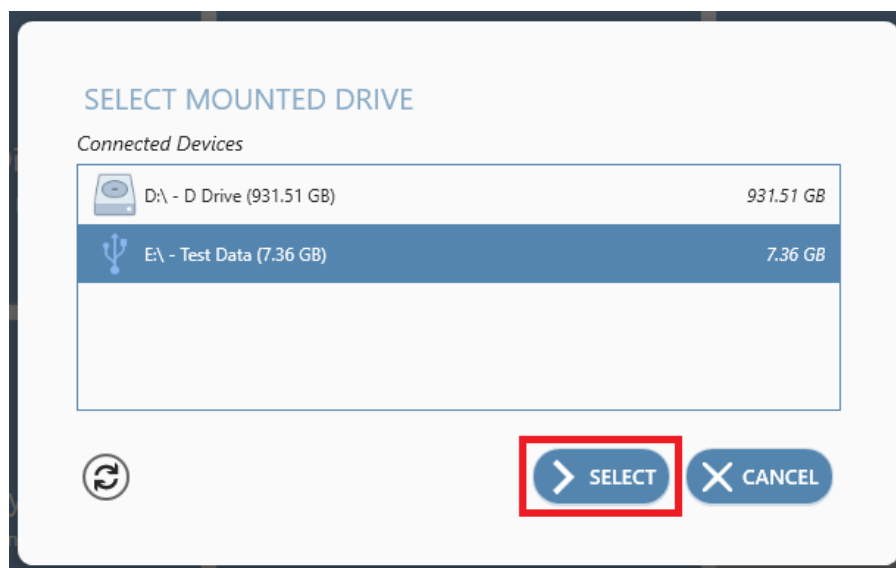
4.5. MOUNTED DRIVE

A Mounted Drive is a storage device (such as a hard drive or CD-ROM) made accessible through the computer's filesystem.

To acquire data from a Mounted Drive, follow the below steps:

- Insert the target media from which you wish to acquire data into the Detego Analyse machine.
 - The 'Auto-Detect' dropdown is irrelevant for a Mounted Drive. If the dropdown displays, close it.
- Select the 'Acquire Connected Media' tile from the Detego home screen.
- Select the 'Mounted Drive' tile.
- From the list of available Mounted Drives, select the one you wish to acquire data from and then click on the SELECT button.

Figure 139



- A Mounted Drive will only allow you to acquire data through a Logical Extraction. You can change the case and exhibit names and descriptions after clicking the SELECT button from the 'Configure Extraction' window.
- You can configure this to your specification and select START or ADVANCED to change the job queue in depth.

Figure 140

Detego Analyse - Configure Acquisition for '02 Dec 2021 11:54:36'

Configure Extraction

Extraction Target

E:\

Case Name : Exhibit Name :

Description :

Logical Extraction

Run job queue when done: ☐

ADVANCED...

START

CANCEL

NOTE! For more information on Jobs; please navigate to the 'Analytics' portion of the 'Analyse and Manage' section within this guide.

4.6. IMAGE FILE

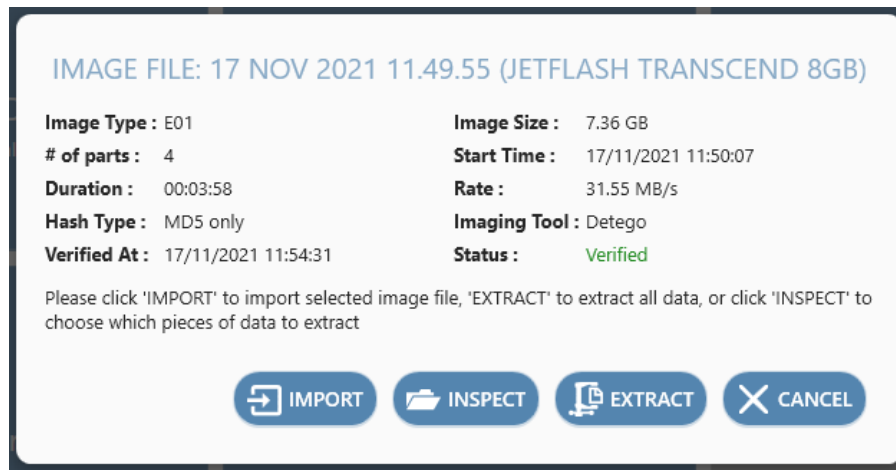
An Image File is a bit-for-bit copy of a device, disk or drive.

To acquire data from an Image File, follow the below steps:

- Ensure the image file is saved onto your Detego Analyse machine or accessible on a piece of removable media.
 - Performance may vary depending on location the image file is saved.
- Select the 'Acquire Connected Media' tile from the home screen.
- Select the 'Image File' tile and browse for the saved image file.

NOTE! The image file must be in an E01, Ex01, DD, Bin or 001/0001 format; VHD and VHDX can also be used.

Figure 141



The above image shows the type of information displayed and gives you the below options you can select:

IMPORT – This will import the image into Detego so you can perform further extraction and jobs later.

INSPECT – This will allow you to inspect the image with Detego Analyse Disk Inspector.

EXTRACT – This will import and extract the image file.

CANCEL – This will cancel the operation.

- Select the **EXTRACT** option to open the 'Configure Extraction' window. After selecting the EXTRACT button, you can change the case and exhibit names and descriptions from the 'Configure Extraction' window.

Figure 142

Detego Analyse - Configure Acquisition for '02 Dec 2021 14:18:36'

Configure Extraction

Extraction Target

G:\exhibits\exhibits\3a003fe8-6939-a4de-b3dd-f2bb7af909e0\Image Data\17 Nov 2021 11:49:55\17 Nov 2021 11:49:55.E01

Case Name : Media Acquisitions Exhibit Name : 02 Dec 2021 14:18:37

Description : Media acquisition from Image file 'G:\exhibits\exhibits\3a003fe8-6939-a4de-b3dd-f2bb7af909e0\Image Data\17 Nov 2021 11:49:55\17 Nov 2021 11:49:55.E01'

Logical Extraction

File Carving

Run job queue when done: ☐

ADVANCED... START CANCEL

- You can configure this to your specification and select START or ADVANCED to change the job queue in depth.

NOTE! For more information on Jobs; please navigate to the 'Analytics' portion of the 'Analyse and Manage' section within this guide.

4.7. DIRECTORY

A Directory is a file system cataloguing structure that contains references to other computer files and possibly other directories.

To acquire data from a Directory, please follow the below steps:

- Ensure that you can navigate to the directory that you wish to acquire. This can be on your Detego Analyse machine or a piece of removable media.
- Select the 'Acquire Connected Media' tile from the home screen.

- Select the 'Directory' tile and then browse to the directory (folder) you wish to acquire data from.
- Once you have selected the directory, the 'Configure Extraction' window will open. After selecting the EXTRACT button, you can change the case and exhibit names and descriptions from the 'Configure Extraction' window.

NOTE! You can only acquire data through a Logical Extraction for a Directory Acquisition.

Figure 143

Detego Analyse - Configure Acquisition for '02 Dec 2021 14:36:12'

Configure Extraction

Extraction Target

E:\Border

Case Name : Media Acquisitions Exhibit Name : 02 Dec 2021 14:36:13

Description : Media acquisition from Directory 'E:\Border'

Logical Extraction

Run job queue when done: ☐

ADVANCED... START CANCEL

- You can configure this to your specification and select START or ADVANCED to change the job queue in depth.

NOTE! For more information on Jobs; please navigate to the 'Analytics' portion of the 'Analyse and Manage' section within this guide.

4.8. MOBILE AND TABLET

DETEGO FOR MOBILE DEVICES - BASIC MOBILE BACKUP

Detego for Mobile Devices allows for very basic mobile backups. Below is a general workflow for using Detego for Mobile Devices, and some devices will vary.

Encrypted backups are not supported, so this should only be used for basic backups.

For full mobile forensics, you will need to install and license our integrated Detego-MD mobile forensic suite. For more information, please get in touch with marketing@detegoglobal.com.

PREPARING ANDROID DEVICES

To acquire from an Android device, follow the below steps:

- In developer options, turn USB Debugging on. To enable developer options, go to settings>about phone>build number, and tap the build number 7 times repeatedly until a notification appears saying developer options are enabled.
- Select USB Debugging mode ON from within developer options and then select Stay Awake mode ON.
- Security Settings require trusting 'Unknown Sources' to enable communication with the software. This setting is located under 'Security' within Settings.
- The USB connection type is viewed within the device's dropdown menu. It can be selected from this window by sliding the screen down from the top and selecting USB Configuration—Media Transfer Protocol.
- Plug the Physical target phone into the Detego machine.

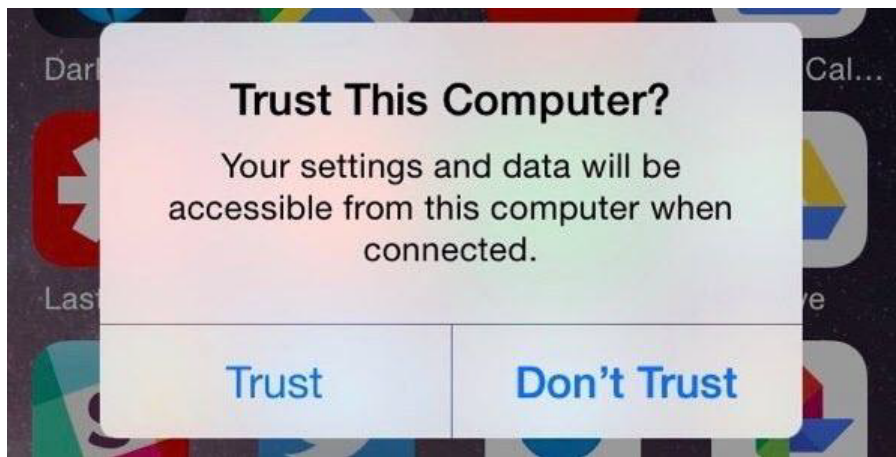
PREPARING IOS DEVICES

To acquire from an iOS device, follow the below steps:

- iTunes must be installed on the system and updated to the latest version.
- Plug the physical target phone into the Detego machine. (Passcode required)

- Trust the device on the iPhone & and follow iTunes prompts.
- Type the passcode into the iPhone. (Disconnect and reconnect if needed.)

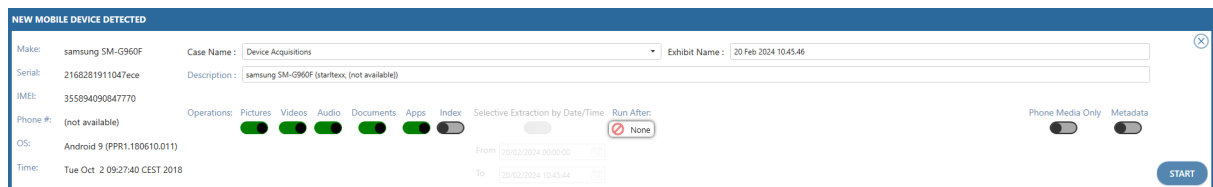
Figure 144



BACKING UP DATA FROM MOBILE DEVICES

When a Mobile device is detected, a dropdown will appear. Basic details about the phone are listed on the left, operations are in the middle, and extra options are on the right.

Figure 145



The available jobs are listed below:

- **Pictures** - This job will extract picture media from the target mobile device.
- **Videos** - This job will extract video media from the target mobile device.
- **Audio** - This job will extract audio media from the target mobile device.
- **Documents** - This job will extract documents from the target mobile device.
- **Apps** - This job will run the app data from the target mobile device after extraction.
- **Index** - This job will index extracted text from the target mobile device after extraction.

- **Selective Extraction by Date/Time** - This job will extract data from the target mobile device within your specified date range.
- **Run After** - This option allows you to run a job queue after the extraction.
- **Phone Media Only** - This is a faster extraction mode that does not complete a full backup and only extracts phone media. It requires that the phone be in MTP connection mode.
- **Metadata** - Allows the user to modify metadata information on the created exhibit.

To perform an extraction:

- Click **START** in the bottom right to initiate the extraction.
- If the device is encrypted, a 'Remove Backup Encryption' message may be displayed once you select START.

'Remove Backup Encryption':

- **REMOVE ENCRYPTION** - If the correct password is added, the encryption will be removed, allowing the jobs to continue.
- **CANCEL** - This will cancel the extraction.

DETEGO MD - ADVANCED MOBILE DEVICE ACQUISITION (POWERED BY GMDSOFT)

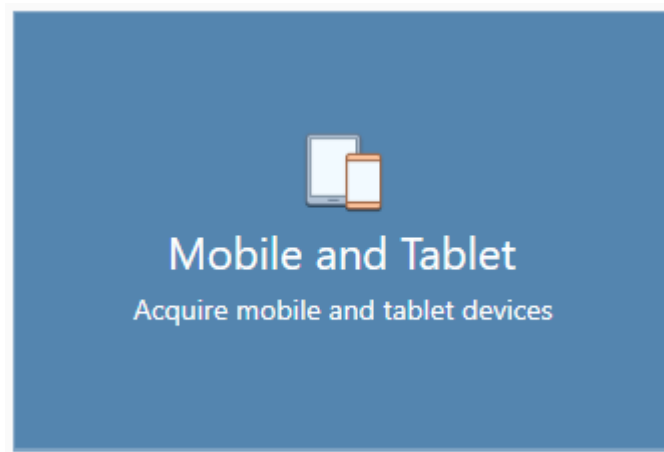
The 'Mobile and Tablet' tile (accessed from the 'Acquire Connected Media' tile on the Home Screen) allows users to acquire data from mobile devices and tablets.

NOTE! You must have Detego MD software installed and licensed to access the 'Mobile and Tablet' tile; otherwise, the tile will be greyed out. Detego MD - our mobile forensic platform powered by GMDSOFT - requires a separate installation and license, so please get in touch with marketing@detegoglobal.com if you wish to learn more.

Follow the steps below to open Detego MD-NEXT:

- From the Detego Analyse home screen, select the 'Acquire Connected Media' tile and then select the 'Mobile and Tablet' tile to open Detego MD-NEXT powered by GMDSOFT.

Figure 146



- Select 'Yes' to any UAC (User Account Control) prompts. This will open the 'MD-NEXT' window. Prior to the UAC prompt, you may be prompted to ensure Detego MD is licensed.

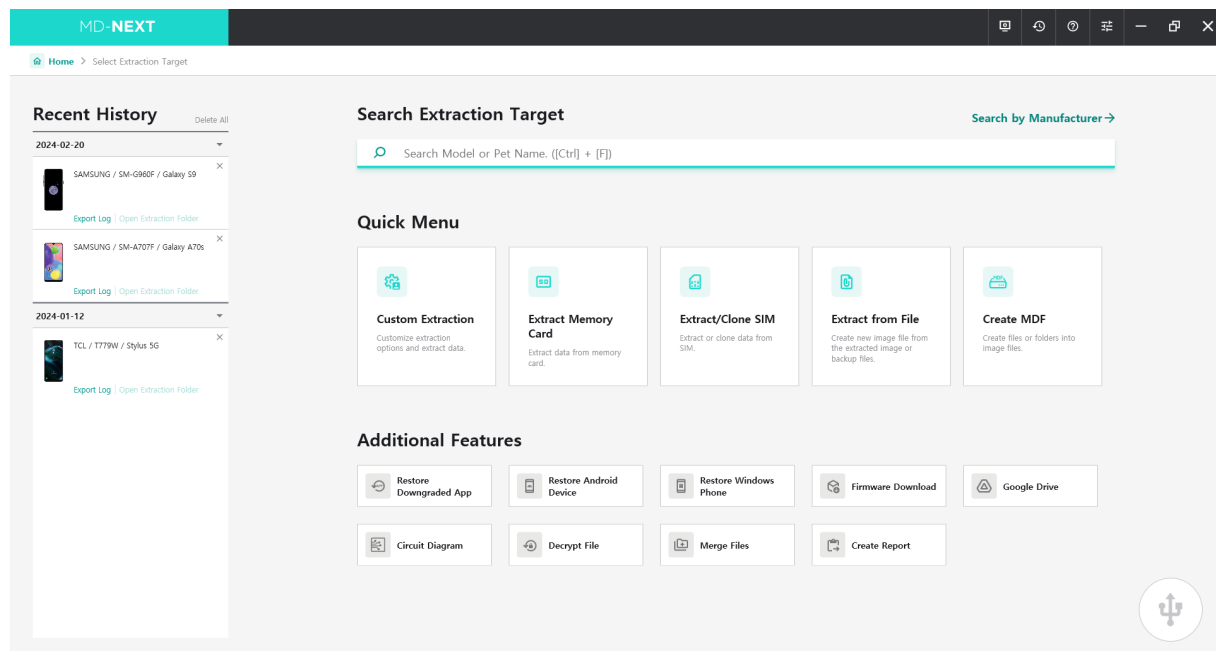
After installation and opening Detego MD NEXT, you may be prompted to choose the default save locations for several data types. We recommend creating folders in a location with a large storage capacity and selecting those when prompted.

You can also use the 'Detego-MD' shortcut that gets placed on your desktop during installation to open the software outside of Detego, but you will need to import it into Detego Analyse before analytics can be run.

DETEGO MD-NEXT HOME SCREEN

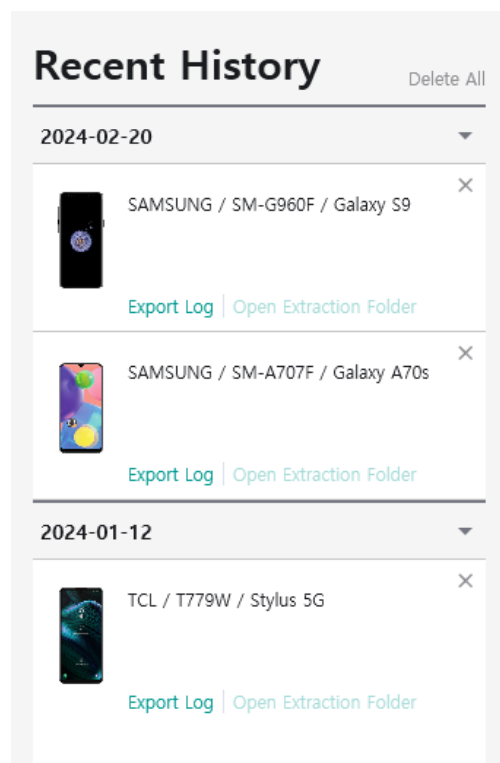
This section will briefly describe the Detego MD-NEXT Home Screen and various actions that can be performed from here.

Figure 147



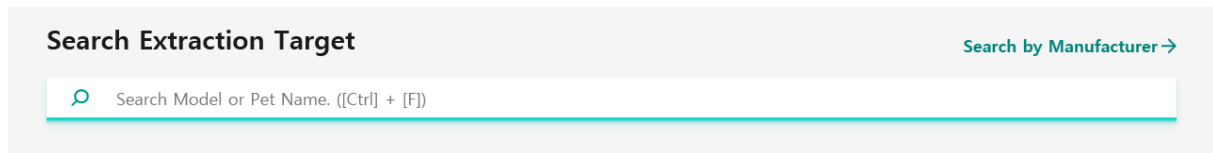
- **Recent History** - This panel on the left displays any recent extractions or searched devices. It allows you to access the Export Log of each device, or if it has been extracted, Open the Extraction Folder.

Figure 148



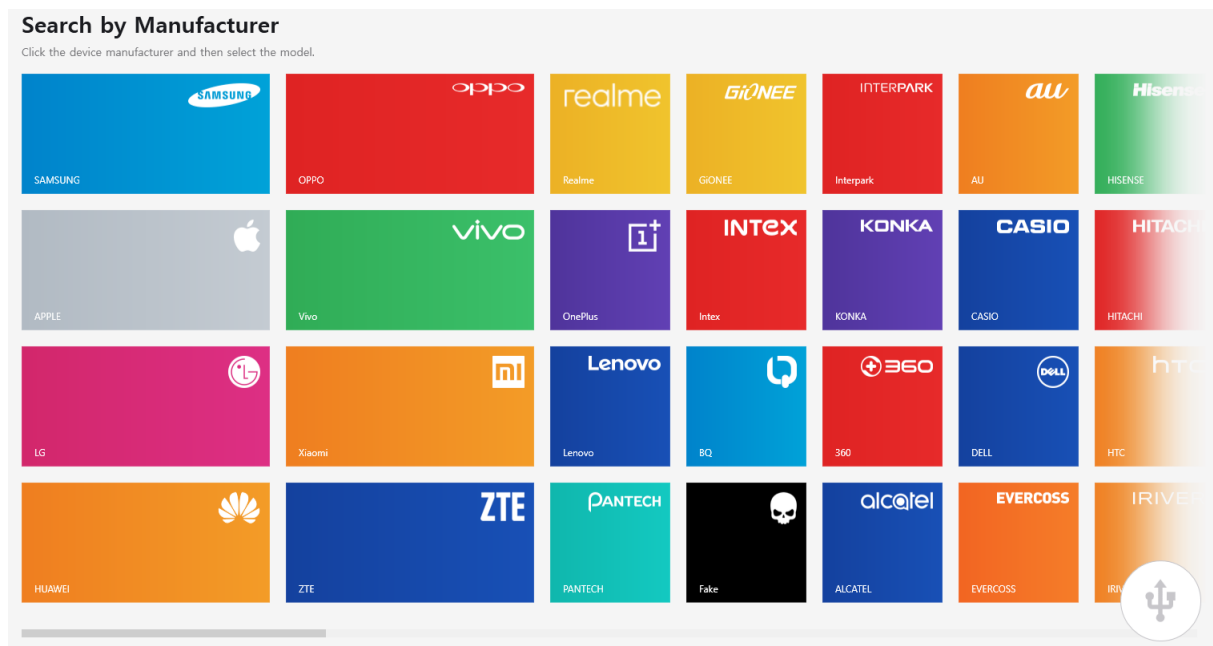
- **Search Extraction Target** - This allows you to search for the model or Pet Name of the device you want to extract from.

Figure 149



- **Search by Manufacturer** - This button takes you to the Manufacturer screen where all supported Manufacturers are listed. (On previous versions of MD-NEXT, this screen would be the Home Screen.)

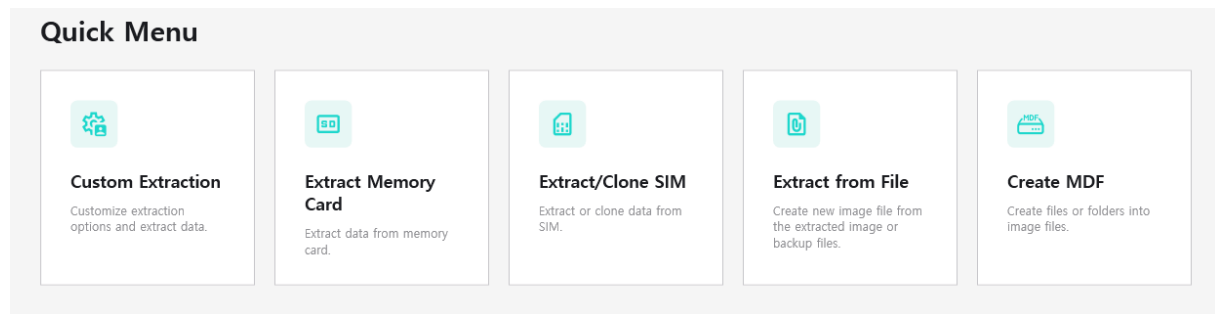
Figure 150



- **Quick Menu** - These options are quick actions you may wish to perform. They include the following:
 - **Custom Extraction** - Customise your extraction options to extract data. This is used primarily when the exact model is not supported or if you are unsure of all the details of the device.
 - **Extract Memory Card** - Extract data from a memory card.
 - **Extract/Clone SIM** - Extract or clone data from a SIM.

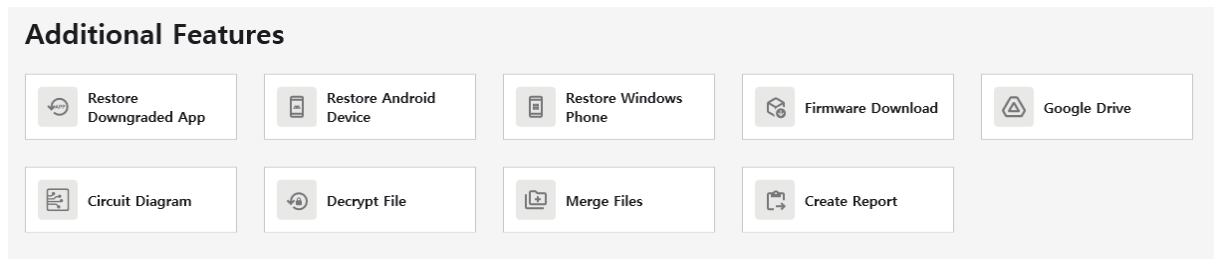
- **Extract from File** - Create a new image file from the extracted image or backup files.
- **Create MDF** - Convert files or folders into image files.

Figure 151



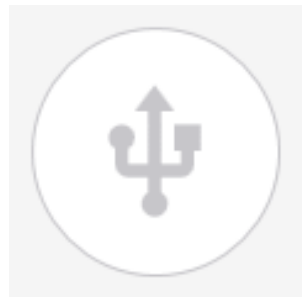
- **Additional Features** - These options are additional actions that can be performed. They include the following:
 - Restore Downgraded App
 - Restore Android Device
 - Restore Windows Phone
 - Firmware Download
 - Google Drive
 - Circuit Diagram
 - Decrypt File
 - Merge Files
 - Create Report

Figure 152



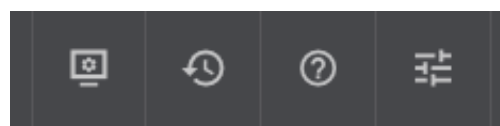
- **Connect Button** - This button in the bottom right corner allows you to detect a device when connecting it to your machine.

Figure 153



- **Toolbar Options** - These are the various options available from the top of the window on the toolbar. These include the following from left to right:
 - **Device Manager** - This opens the Windows Device Manager window.
 - **Log** - This opens the Log window where you can check the logs of the software.
 - **Help** - This opens the Help window, which displays the MD-NEXT version number, the available Quick Links and your current License Details.
 - **Settings** - This opens the Settings window.

Figure 154



DETEGO MD-NEXT - EXTRACTIONS

This section will only cover a basic extraction of devices and import into Detego Analyse. The following documents (found within the Help section of MD-NEXT) will cover more information:

- **Supported List** - This is a spreadsheet with a full list of supported devices and the available extraction methods for each device.
- **User Guide** - This is the full MD-NEXT User Guide with further information and details on the software.
- **Troubleshooting Guide** - This guide will assist you with any connectivity issues or various problems you may encounter.

Figure 155

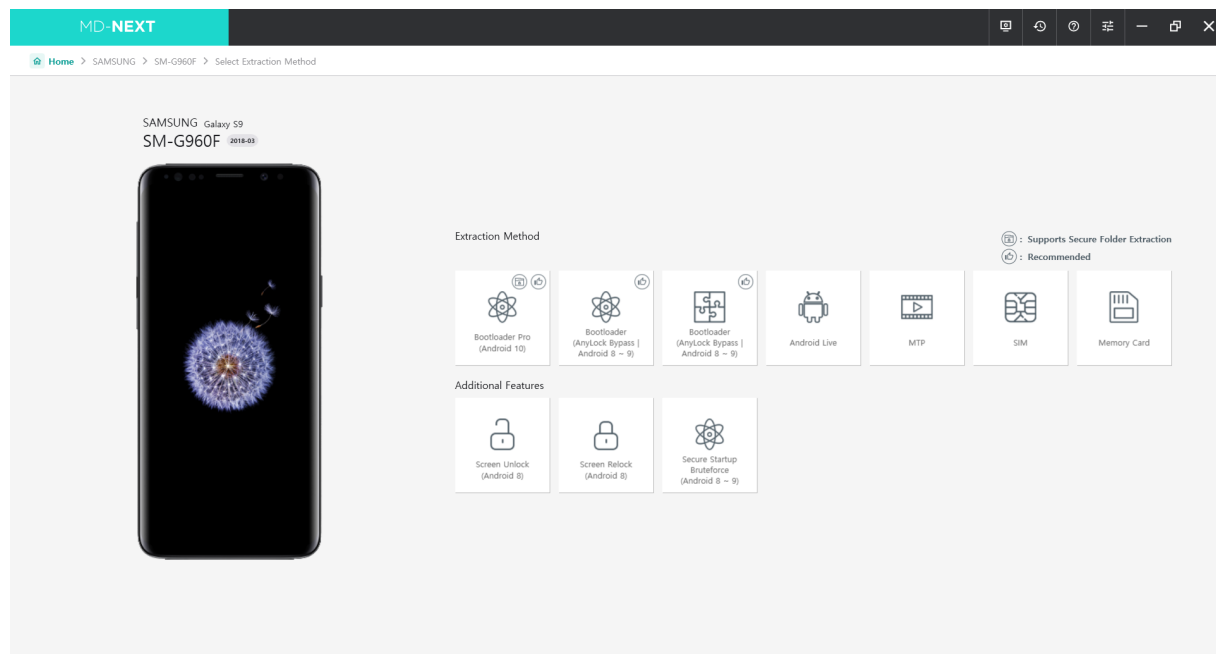


EXTRACTION OF SPECIFIED/SELECTED DEVICE

Once you have located a device you wish to extract from, you will be able to select an extraction method from the screen below.

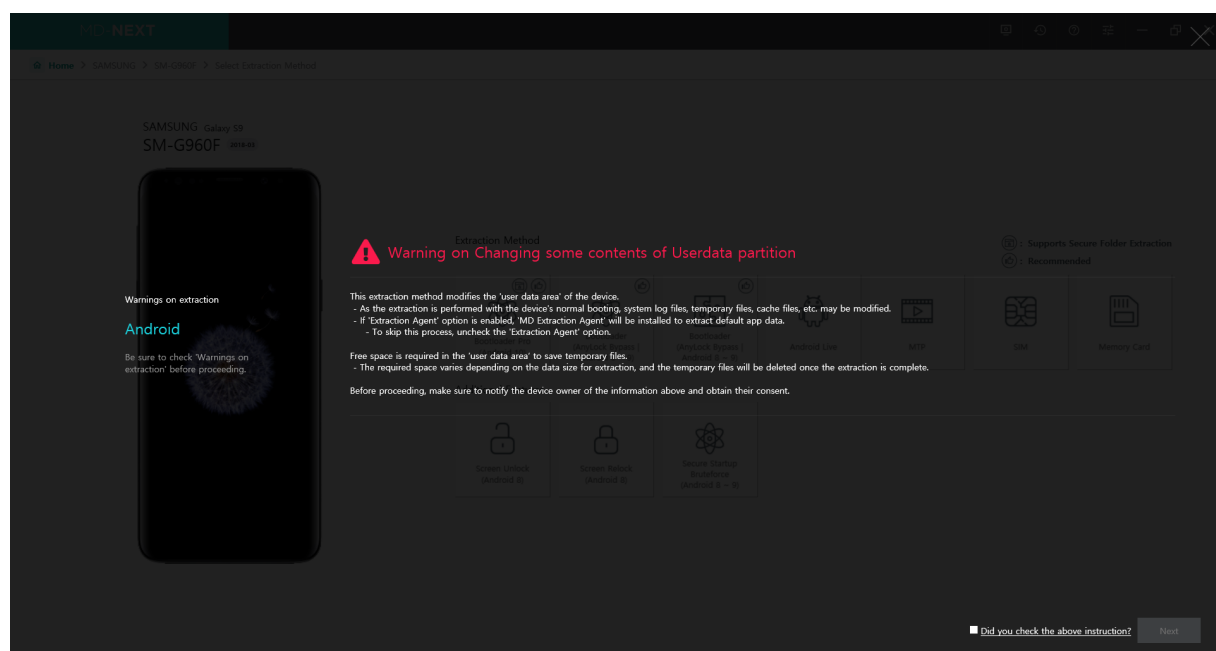
NOTE! The available extraction methods will vary depending on the device, model, OS, OS version and MD-NEXT version.

Figure 156



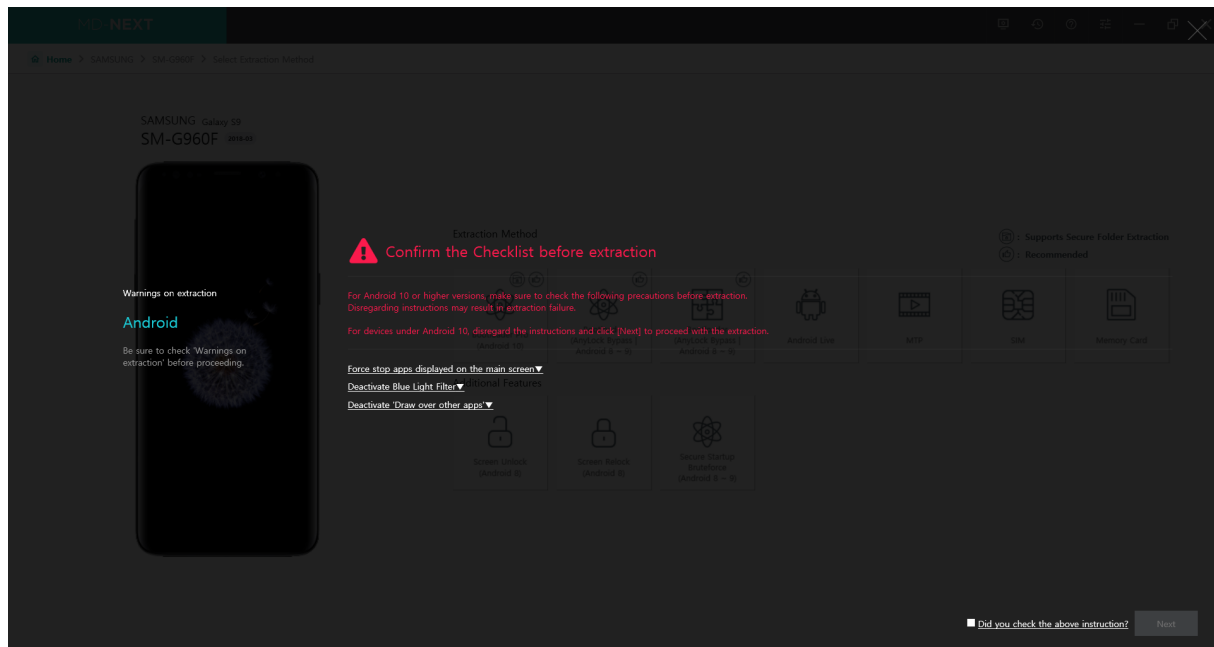
- Select your extraction method. For this example, we have selected Android Live, which is a Logical Extraction.
- Read through the warning prompts that appear, and when you are happy, tick the checkbox before selecting Next.

Figure 157



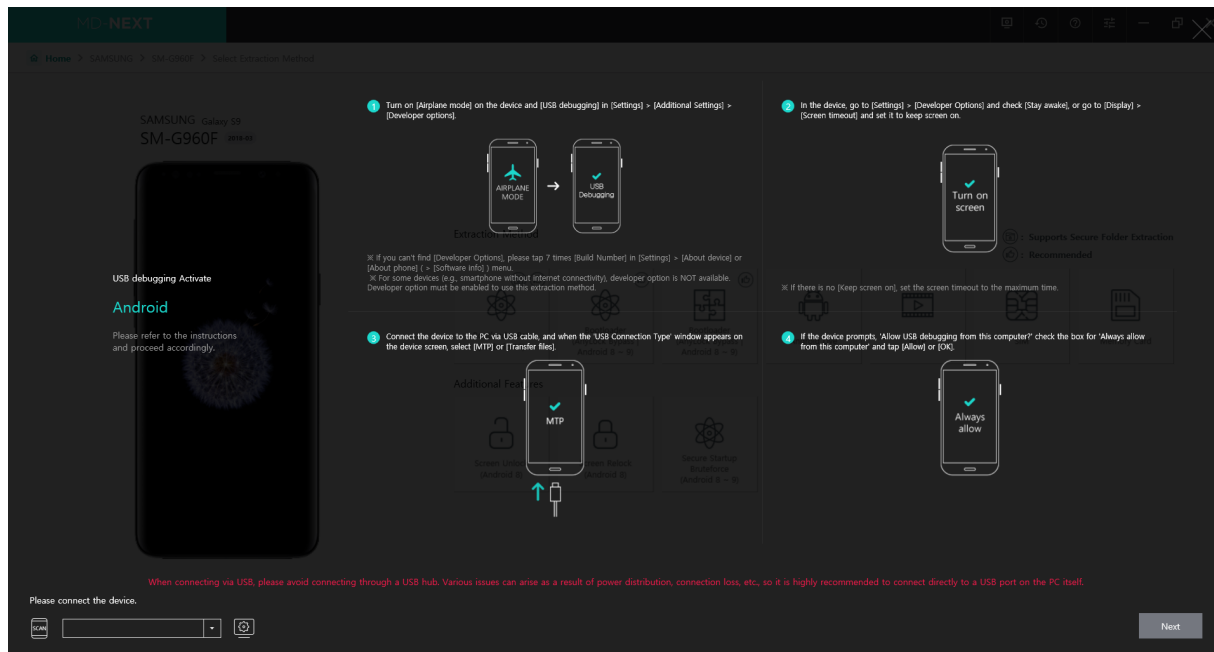
- Please read through the next prompt (if applicable) and follow any relevant steps if necessary. Then, tick the checkbox before selecting Next.

Figure 158



- Follow the steps carefully on the next screen to ensure successful connection and extraction. Ensure all steps are followed on the screen and the device to prevent issues.
- Once you follow the steps, you may need to unplug and reinsert the device again before selecting the SCAN button at the bottom left of the screen.
- Once you have selected SCAN and the correct device is selected in the dropdown list, select Next.

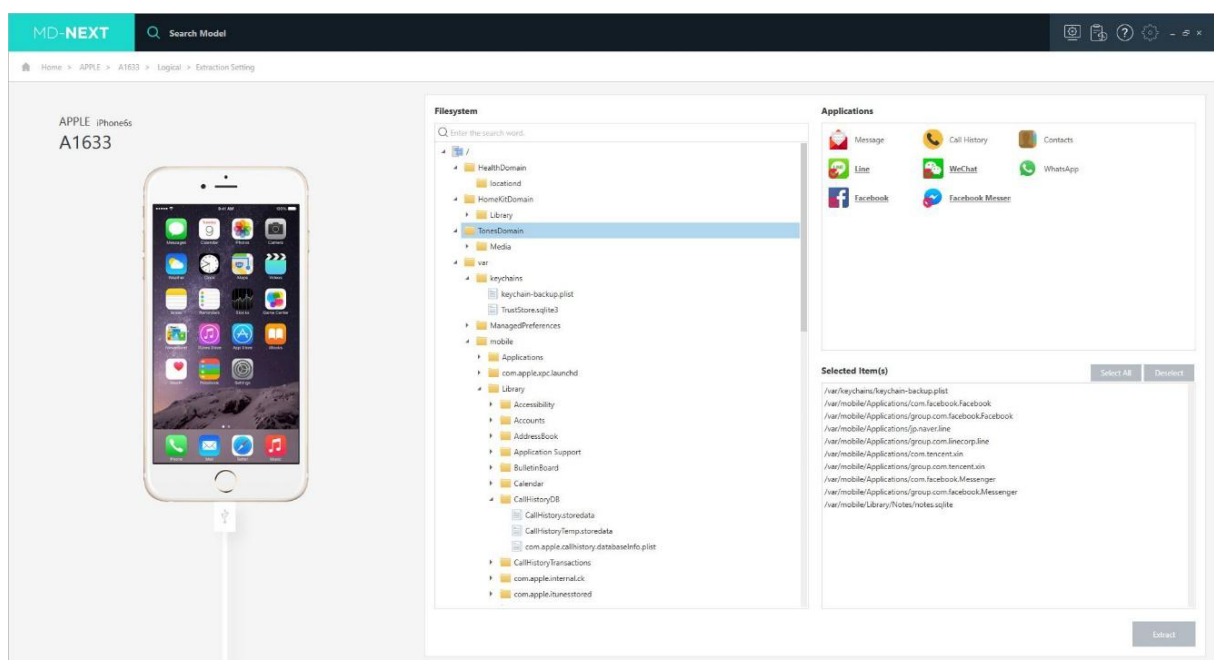
Figure 159



- Enter a password for backup if desired.
- You will have two options, 'Extract All' or 'Select Extraction'. Selecting an extraction option will display the screen below. You can select single applications or files within the file structure for extraction.

NOTE! UI may vary slightly in the latest release.

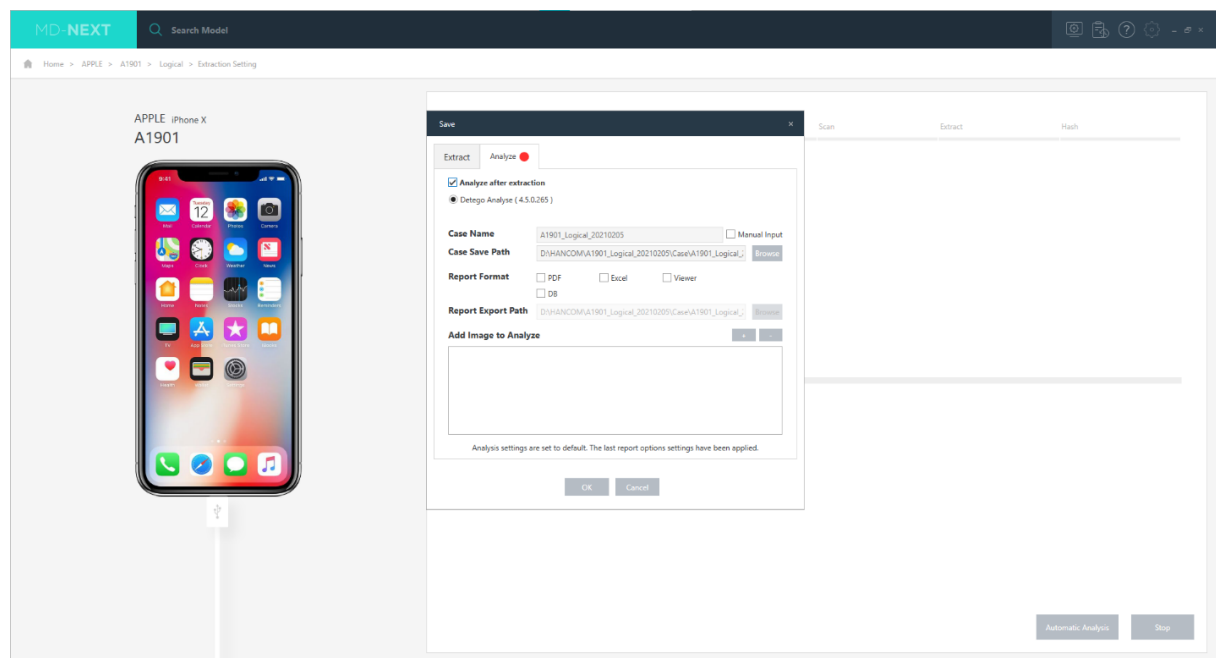
Figure 160



- Select 'Next' to open the 'Saving' pop-up.
- Tick the 'Analyse with Detego' option under the Analyse tab and select 'OK' to run the extraction. This will automatically import the MDF into Detego Analyse and then run the MD RED processes in the background of Detego.

NOTE! UI may vary slightly in the latest release.

Figure 161



NOTE! The MDF Importer can be used if MD-NEXT has acquired an MDF file but has not performed an analysis. It is useful if you extract and forget to select the 'Analyse with Detego Analyse' option within MD-NEXT.

Please see the 'Analytics' section to find out more.

WARNING! If you wish to complete a Bootloader Extraction, you do not need to be connected to the internet to download firmware; however, if your phone has broken or become stuck, it is recommended that you download the firmware to reflash it.

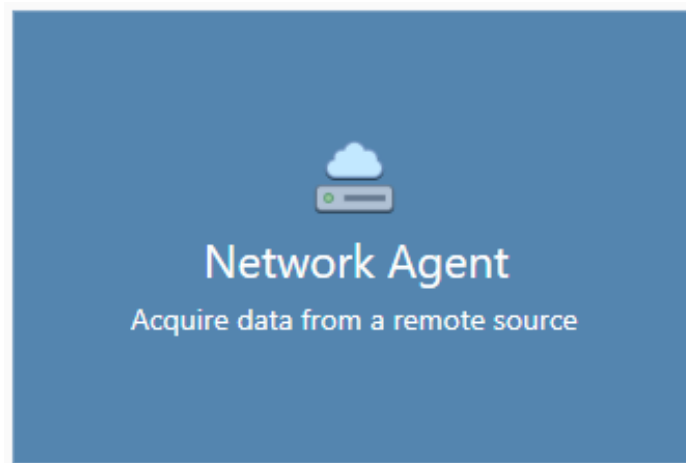
- Select the device you wish to extract and download the .zip file.
- Once downloaded, you must place this file into the 'Firmware' folder you selected when you first installed it (this can be checked and changed in the MD-NEXT settings).

- You can now complete a bootloader extraction for your specified and downloaded device.
- Samsung and Oppo bootloaders and Custom Images are available from our installation Manager.

4.9. NETWORK AGENT

The Network Agent tile allows acquiring data from a remote target machine. Please be aware this is an add-on feature and requires additional setup and System Administrator steps to run correctly. For more information, please contact marketing@detegoglobal.com.

Figure 162



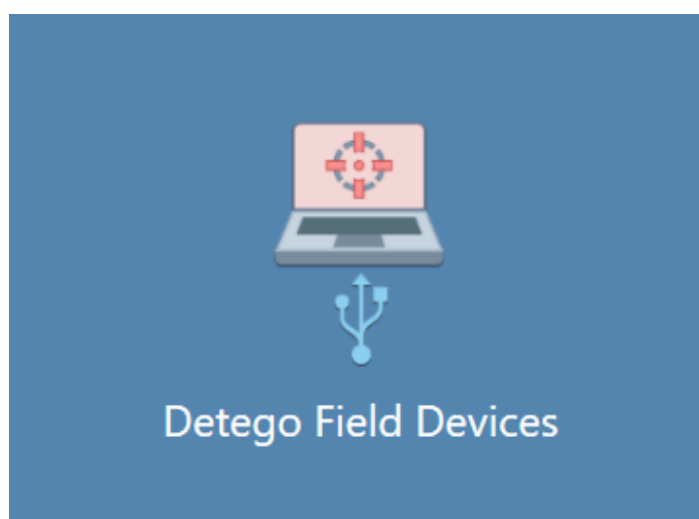
Information on setting up Network Agents and acquiring data from remote sources can be found in the Remote Acquisition User Guide. The guide can be located on your desktop after installing Detego Analyse or from the Secure Customer Portal.

5. DETEGO FIELD DEVICES

Detego Field is the on-site extraction functionality used to extract from a Windows, Mac or Linux device.

Detego Field does not require installation on the target device as it runs externally from a licensed Field device. This will result in no noticeable changes to the target device.

Figure 163



Once the data has been extracted through Detego Field, it is imported into Detego Analyse, where analytics can be done and reports generated.

5.1. DETEGO FIELD CHANGE LIST - DISCLAIMER

When using a Detego Field Device to extract a target machine for a LIVE extraction, please be aware the below list are items that Windows may create during insertion of the Detego Field Device or during extraction.

Note: These changes are in relation to Field Extractions within the Live Environment.

These changes are minimal but are listed below for your records.

USB REGISTRY ENTRIES

- HKEY_LOCAL_MACHINE\system\controlset001\
- HKEY_LOCAL_MACHINE\software\microsoft\windows nt\currentversion\emdmgmt\

- HKEY_LOCAL_MACHINE\software\microsoft\windows portable devices\
- HKEY_LOCAL_MACHINE\software\microsoft\wbem\wdm\dredge\
- HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices\
- HKEY_USERS\s-1-5-21-4169746326-1296783801-3038343627-1001\software\classes\localsettings\software\microsoft\windows\shell\muicache
- HKEY_USERS\s-1-5-21-4169746326-1296783801-3038343627-1001\software\microsoft\windows\currentversion\explorer\mountpoints2\
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
HKEY_USERS\S-1-5-21-3252640446-386100537-755982263-1001\Software\Microsoft\Windows\Shell\BagMRU\0\0\0
- HKEY_USERS\S-1-5-21-3252640446-386100537-755982263-1001\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store

For versions on WinXP

- HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatibility\AppCompatCache

For versions above WinXP

- HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache\AppCompatCache

PREFETCH %SYSTEMROOT%\PREFETCH

- D_ENGINE.EXE*
- D_CONFIG.EXE*
- CONFIG.EXE*
- RUN.EXE*
- BOOK.EXE*

JUMPLISTS (SPECIFICALLY EXPLORER)

- C:\Users\User\AppData\Roaming\Microsoft\Windows\Recent

LOG FILES

- C:\Windows\inf\setupapi.dev.log

This file is modified before anything is mounted as it logs the driver installation for the USB device. This could change for a whole factor of reasons such as type of external storage device ID.

- EventLogs = \Windows\System32\winevt\Logs
- DeleteFileOnReboot(driveletter + @"\hiberfil.sys", log);
- DeleteFileOnReboot(driveletter + @"\pagefile.sys", log);
- DeleteFileOnReboot(driveletter + Properties.Resources.EventLogs + @"\Microsoft-Windows-DriverFrameworks-Usermode%4Operational.evtx", log);
- DeleteFileOnReboot(driveletter + Properties.Resources.EventLogs + @"\Microsoft-Windows-Kernal-Pnp-Configuration.evtx", log);

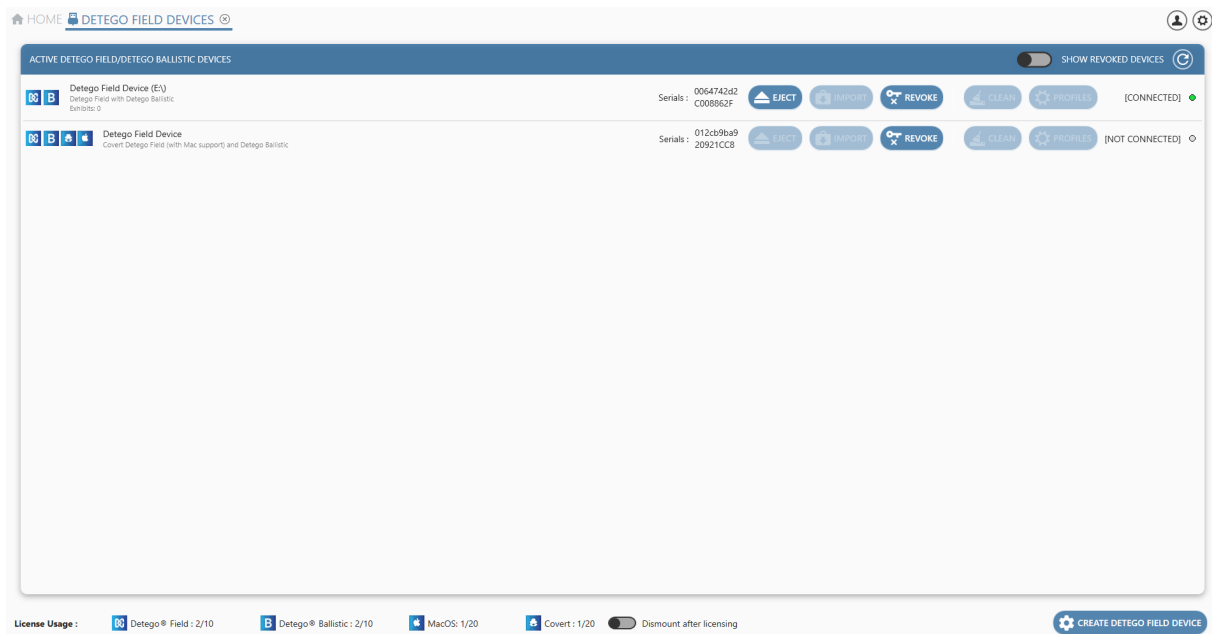
5.2. LICENSING FIELD DEVICES

To utilise Detego Field, you must license your Detego Field devices to store the Detego Field software and configuration tools (including Detego Ballistic Imager, if applicable).

Detego Field and Ballistic Collector devices should be formatted as exFAT for speed and efficiency.

From the Detego Home Screen, select the “Detego Field Devices”. This will bring you to the Detego Field Devices screen and display your currently licensed devices.

Figure 164



To license a new Detego Field Device, follow the steps below:

- Insert a blank USB 3.0 device. We recommend manually wiping it and formatting it as exFAT; however, Detego will correctly format it. It's recommended to use fast and reliable USB 3.0+ devices with a lot of storage to allow for quicker extractions.
 - *(High performance SSDs and NVMe drives are recommended due to high performance and capacity.)*
- You will be presented with a list of all your active Detego Field and Ballistic devices. The active devices connected to your machine will have a 'Connected' message next to them, and disconnected ones will display 'Disconnected'.
- You can view revoked licenses by toggling the 'Show Revoked Devices' field at the top of the window. Toggling this can take a while for changes to take effect.
- You can monitor your Detego Field, Detego Ballistic, Covert and Detego Field for MacOS license usage at the bottom of the window. The denominator shows the number of licenses you purchased, and the numerator shows the number of licenses you have already licensed to Field devices.
- Select the 'CREATE DETEGO FIELD DEVICE' button in the bottom right corner to create a new Detego Field Device.

- Select the removable drive you want to license from the 'New Detego Field Device' window dropdown. You can name your Field device and select which Detego features you want to license the device. These options are Detego Field, Detego Ballistic Imager, Detego Field for MacOS and Covert.
- Please note that some of these options will effect how the Field Configuration looks later in this manual. For example if Covert is applied you will have the option to run your Profile in Covert. The images used in the manual have all options active as an example.

Note: Only devices with a valid serial number and at least 2GB of storage can be licensed. Some budget USB devices don't have serial numbers, and Detego Analyse may not detect them (we also do not advocate using cheap USB devices from a longevity, heat management and reliability perspective).

HDDs (Hard Disk Drives/spinning platter drives) are not supported as Field devices, and you may experience issues during licensing or extraction. Speed will be significantly reduced.

CAUTION! Licensing a Detego Field device will format it, and you will lose all existing data.

Figure 165



5.3. DETEGO FIELD LEGACY - WINDOWS 7 COMPATIBLE

The Detego 'Legacy Field' is an option that allows for compatibility with older versions of Windows 7 devices and should only be used if the Detego Field Live environment does not work on the Windows 7 machine or if the Detego Field Boot Environment is not suitable.

You must download the 'Legacy Field' .zip file from the Installation Manager or our secure portal.

If you install via the Install Manager, you do not need to do anything once installed. The installation of the Legacy Field within the Install Manager places the file in the correct location.

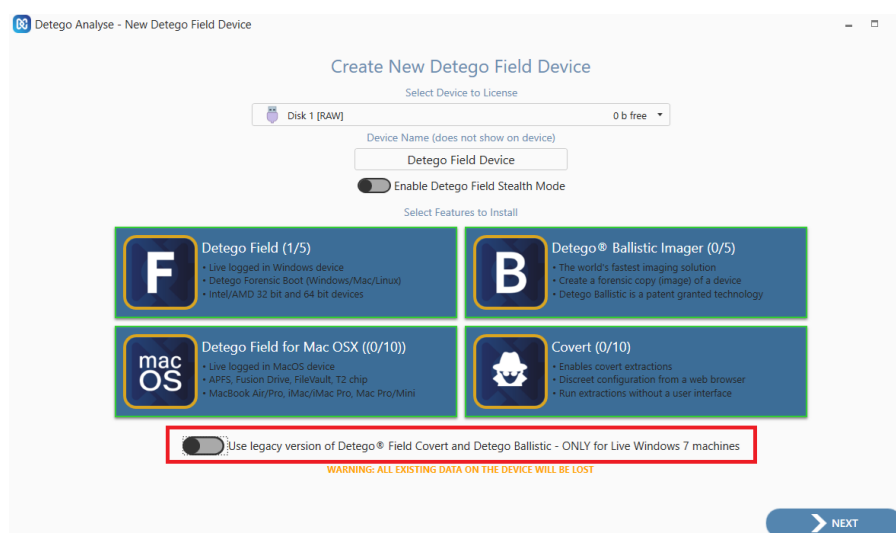
If you have downloaded the 'Legacy Field' file from the secure portal, you will need to follow the steps below to install Legacy Field:

- Download the 'Legacy Field' .zip file from our secure customer portal
- Place the file in the path: C:\ProgramData\Detego

Please note that the 'ProgramData' folder is hidden by default, and you will need to enable 'View hidden items' from the View menu within File Explorer.

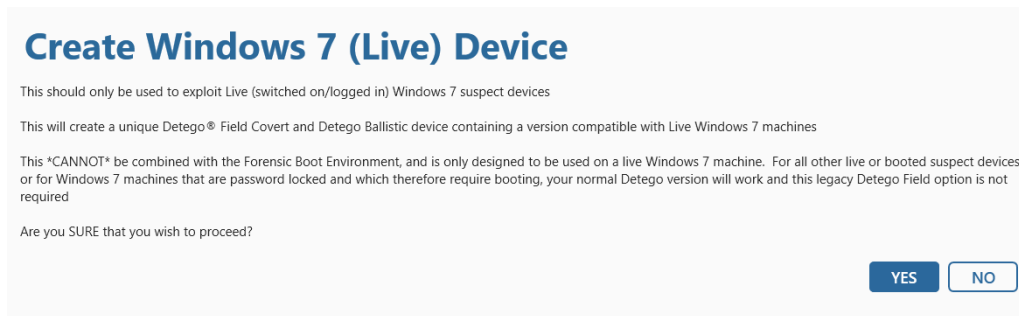
- Close Detego (if open) and restart the 'detegosrv' service from the task manager.
- Once this process is done, you should see the toggle button below when licensing out a Field device.

Figure 166



- Select the toggle button to create the Legacy Field device for Detego Field, Detego Ballistic or Covert. This will vary depending on which options you have selected. This feature is not relevant for Detego Field for MacOS.
- The confirmation prompt below will be displayed, read carefully, and select YES if happy.

Figure 167



- Once you have selected YES, you will see the below message in the top right corner of the Field licensing window as a warning/reminder that you are creating it for Windows 7 LIVE mode only. WARNING! Some features in this guide may not be available for a Legacy Field device.

Figure 168



5.4. LICENSING BOOT DEVICES

Detego Boot Environment is a 64-bit version that should be compatible with most 64-bit and 32-bit Operating Systems. A Legacy Boot Environment that supports older 32-bit Operating Systems is available on request.

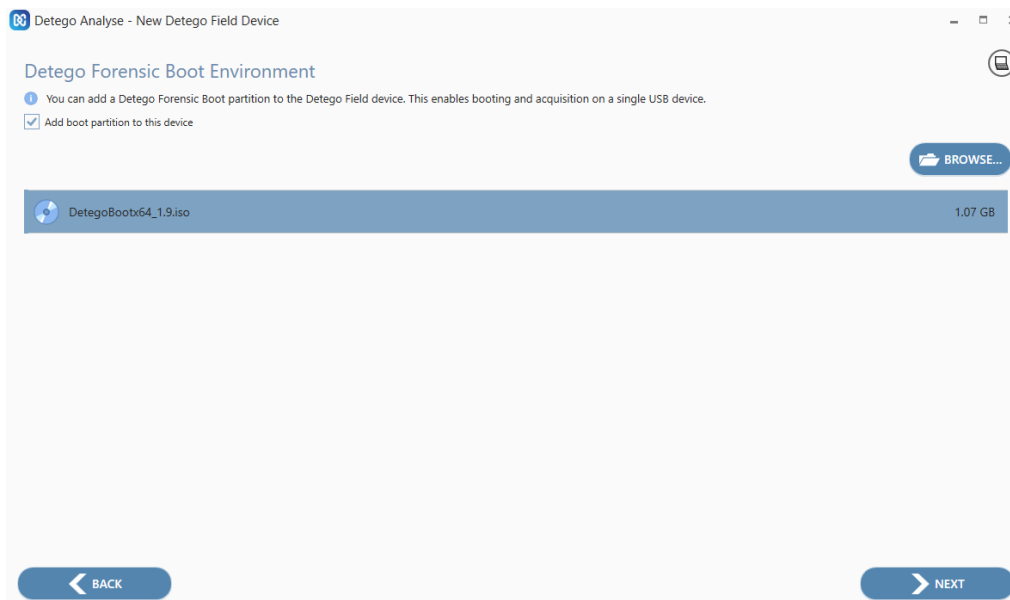
Detego Boot Environment can only be run with the supplied .ISO files bundled into our 'Detego Boot Environment' .zip file available from our Install Manager or our secure customer portal.

Detego Boot Environment can be included and run from the same licensed Field device. Follow the below:

- Select the 'Add boot partition to this device' checkbox.

- Browse to the downloaded 'DetegoBootx64.iso' if not previously added.
- Select NEXT to add the boot partition and move on to the next section.

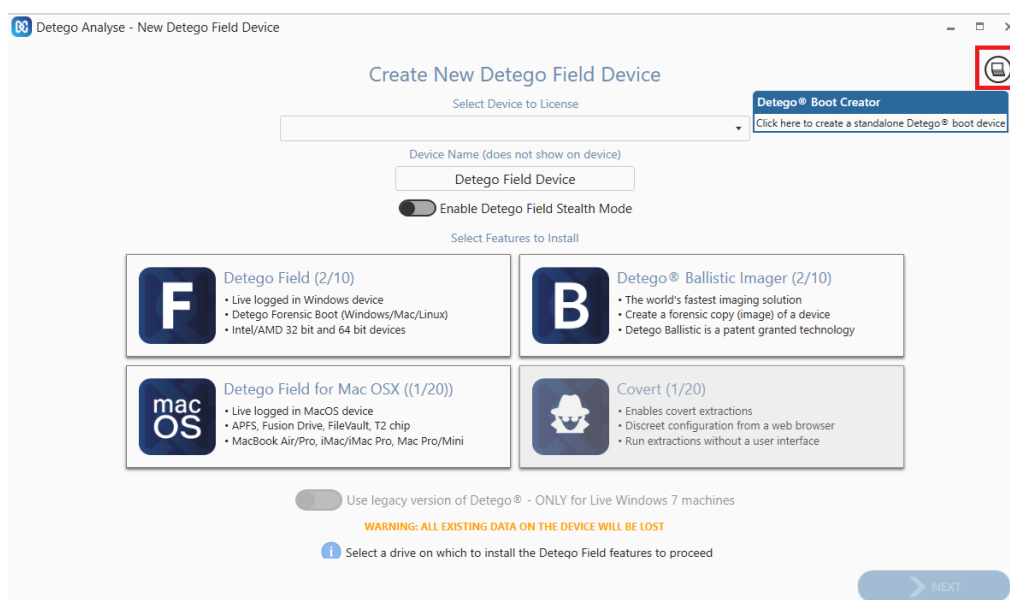
Figure 169



If you wish to create a Detego Boot device that is not a Field device, please make sure the Boot Creator has been installed via the Install Manager.

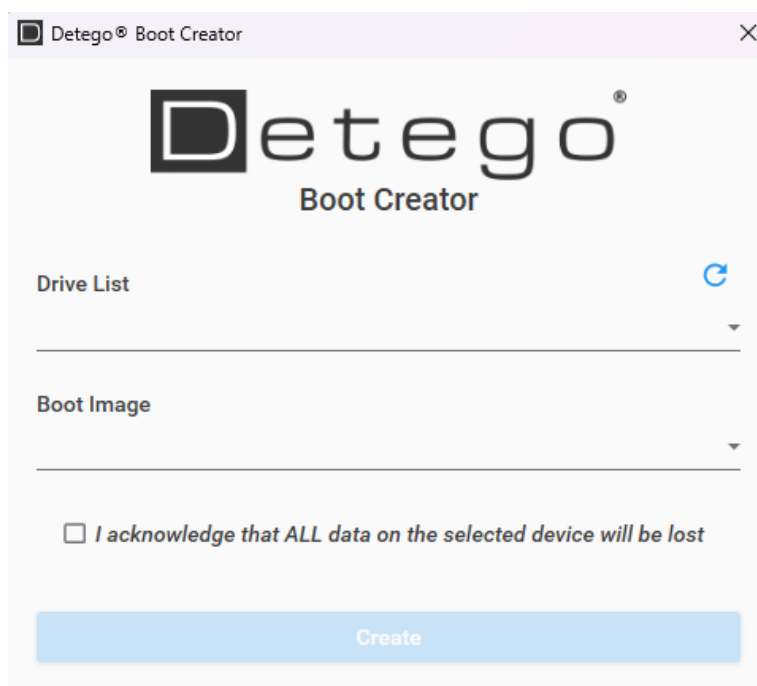
A button is available on the Create New Detego Field Device dialog box, allowing the boot creation tool to be started when installed:

Figure 170



When pressed this opens the Boot Creator program, allowing standalone boot devices to be created that can start Detego Field on hardware which does not support using an integrated boot partition:

Figure 171



5.5. ADDING HASHLISTS AND KEYWORD / REGEX LISTS

To get "quick hits" extractions from target devices, you can add Keyword Lists and Hashlists to your Detego Field device. You can add these lists if you have already created them within the CONFIGURATION of Detego Analyse.

- Within the 'New Field Device' window, you can select the 'NEW HASHLIST' to create a new Hashlist or 'NEW KEYWORD/REGEX LIST' to create a new Keyword/regex list if you haven't created one within Analyse.

Figure 172

The screenshot shows a software window titled "Detego Analyse - New Detego Field Device". It contains two main panels for selecting lists. The left panel, titled "AVAILABLE HASHLIST", has a checkbox at the top and a list of four hashlists: "Borders (12,797)", "C T (24)", "IIOC (42)", and "Police (20)". Each item has a checkbox and a circular icon with a plus sign. Below this list is a "NEW HASHLIST" button and a text input field labeled "Hashlist Encryption Password (Optional)". The right panel, titled "AVAILABLE STANDARD/REGEX LIST", also has a checkbox at the top and a list of eight items: "[PREINSTALLED] Cryptocurrency (78)", "[PREINSTALLED] Encryption (70)", "[PREINSTALLED] IED & Precursor (89)", "[PREINSTALLED] Borders (47)", "[PREINSTALLED] Cloud Apps (21)", "[PREINSTALLED] P2P Apps (28)", "IIOC Regex (5)", and "Keyword List 1 (4)". Each item has a checkbox and a circular icon with a plus sign. Below this list is a "NEW STANDARD/REGEX LIST" button. At the bottom of the window are "BACK" and "NEXT" buttons.

Note: Using Keyword lists/Hashlists during Field acquisition will allow real-time triage with red, amber and green traffic light signalling to indicate hash or keyword matches in your data.

- Select the checkbox next to the Keyword/regex lists and hashlists you wish to license out from the list, and then SELECT NEXT when ready to move on.
- The 'Hashlist Encryption Password' Optional box will allow hashes to be password-encrypted on the Detego Field device. This will ensure others cannot read them if a Detego Field Device is lost. When running an extraction containing a protected hashlist, you will be prompted to enter the password or run without using that hashlist.

Figure 173

This is a close-up of the "Hashlist Encryption Password (Optional)" section. It features a text input field with a light blue border and a light blue shadow, set against a light gray background.

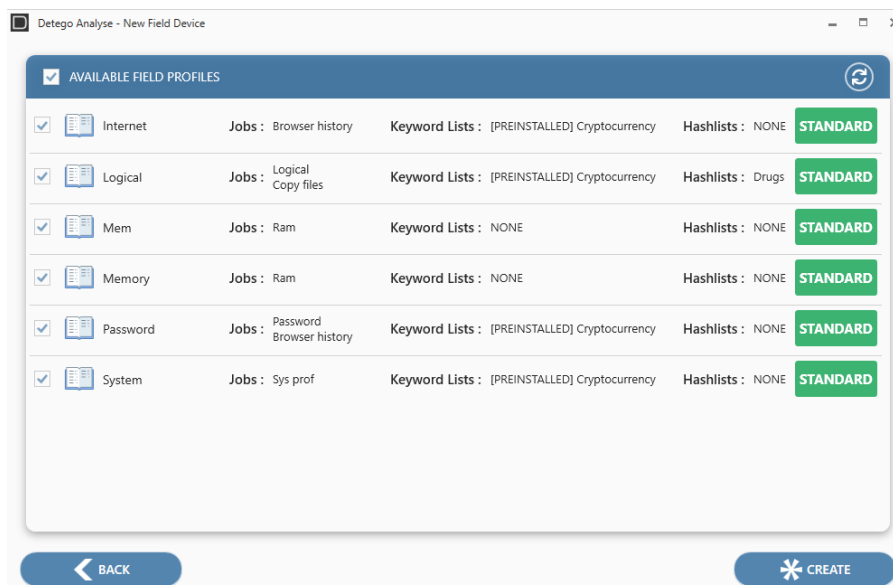
5.6. ADDING FIELD PROFILES

You must have configured some Detego Field Profiles and imported them into Detego Analyse. Once you have imported these Profiles, you can create a Detego Field Device with the profiles selected.

To do this:

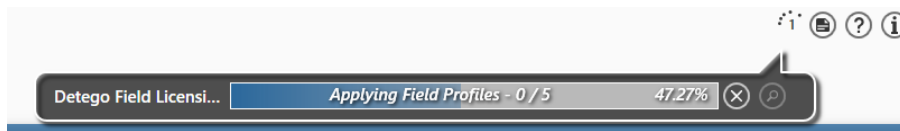
- Check the profiles you wish to add to the Field Device you are licensing.
- On the right side of the profiles, a button will read 'STANDARD' or 'RUN DIRECT'. You can only select this button to toggle between the two [2] options within Detego Configuration.
 - **STANDARD** – This will act like a saved profile.
 - **RUN DIRECT** – This will create a .exe file similar to the 'Run' program file, which allows running the profile directly from the root of the folder. (This is a 'Profile Creator' .exe)

Figure 174



- Once you are happy with your selection, select the CREATE button in the bottom right corner of the Detego Field Creation window. The below message will appear in the top right corner to display the job's progress.

Figure 175



5.7. CREATING ADDITIONAL BALLISTIC COLLECTORS

Additional Collectors for Detego Ballistic Imager are useful if needing to image large drives. To create additional collectors, a seed file must be copied onto each additional collector drive (USB/SSD) for Detego Ballistic Imager to recognise them.

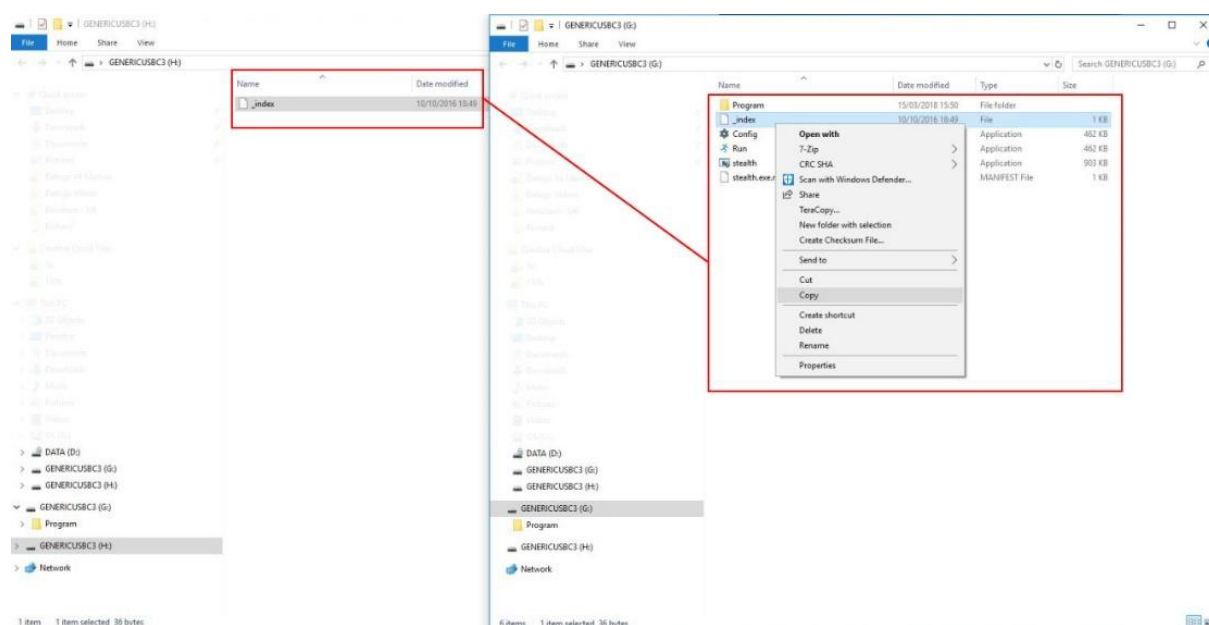
NOTE! All Detego Field devices and Detego Ballistic Collectors must be formatted as exFAT.

To copy the seed file, follow the steps below:

- Insert your fully licensed Detego Ballistic Imager Master device into your machine and navigate to the device in File Explorer. Detego would have named it 'GENERICUSB' unless you renamed the device.
- Open the USB device in File Explorer to reveal its contents.
- Copy the seed file named '_index'. (You can paste it to your desktop if your machine has limited ports.)
- Insert your Detego Ballistic Collector into your machine.
- Open each collector within File Explorer and paste the seed file into the root folder of each collector.

The new devices are now Ballistic Collectors.

Figure 176



5.8. RUNNING DETEGO FIELD ON WINDOWS AND MACOS

The following sections for Detego Field will cover running the Detego Field tool on both Windows and MacOS. Some jobs that are available on Windows may not be possible on MacOS and shall be noted where appropriate.

DETEGO FIELD FOR WINDOWS

Insert the Detego Field (for Windows) device into the Windows machine you wish to target.

The contents of the Field device will appear on the screen. Otherwise, navigate to 'My PC' and double-click on your Field device. Detego will have named the drive 'GENERICUSB' or similar unless specified otherwise.

Note: Make sure to run any of the following as an 'Administrator' to avoid any potential problems. For this, please use the Admin User Account on the target machine or have the admin password to hand when launching on a Standard User Account, as this will be required when launching the files in 'Administrator'. To run as administrator, simply right-click the file and select 'Run as Administrator'.

The following files should be identifiable:

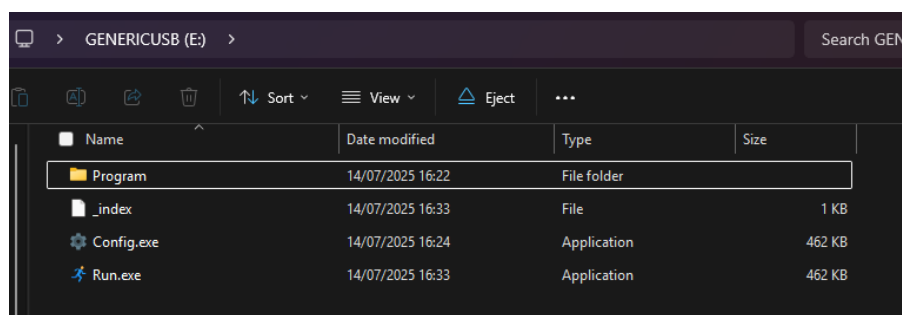
- **Config.exe** – Open the 'Detego Field Config' screen

- **Run.exe** – Instantly runs an acquisition using the last configured profile.
- **Program Folder** – Contains all the files Detego Field needs to run, for example, Profiles, Resources, Tools, and log files.
- **_index** - The seed file for Ballistic collectors.

If Covert has been licensed, these two options will also be visible:

- **Book.exe** – Runs Detego Field, disguised within a flight booking page.
- **stealth.exe** – A small program that removes traces of Detego or the Field Device USB from the Windows registry. If Stealth.exe runs, the clean-up is triggered once the Field Device is removed from the machine.

Figure 177



DETEGO FIELD FOR MACOS

Insert the Detego Field (for MacOS) device into the MacOS machine you wish to target.

NOTE! Make sure to run any of the following as an 'Administrator' to avoid any potential problems. For this, please use the Admin User Account on the target machine or have the admin password to hand when launching on a Standard User Account, as this will be required when launching the files in 'Administrator'. To run as administrator, simply right-click the file and select 'Run as Administrator'.

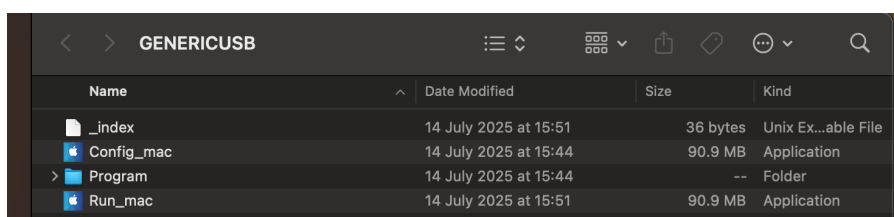
The following files should be identifiable:

- **Config_mac** - Open the 'Detego Field Config' screen where the target is an Apple Mac
- **Run_mac** – Instantly runs an acquisition using the last configured profile where the target is a Mac

- **Program Folder** – Contains all the files Detego Field needs to run, for example, Profiles, Resources and Tools.
- **_index** - The seed file for Ballistic collectors.

Once the user has inserted the Detego Field device, right-click 'Config_mac' and click 'Run as Administrator' to access the configuration menu. **NOTE! Some features may be unavailable if you use the Detego Field for Mac on a Mac device.**

Figure 178



NOTE! When running Detego Field on MacOS, you will be prompted for the user's password. Enter this if it is known; if not, enter the WRONG password three times, and you will progress with less targetable data.

MACOS SUPPORT

This section details current support for MacOS devices. Note the security limitations when targeting MacOS, and refer to the MacOS Support Flowchart, the MacOS Support Table, or the lists below (see important footnotes):

NOTE!

- Detego Analyse 2026.2 supports logical extraction of Ballistic (E01) APFS forensic images from macOS targets (non-chipped), in addition to the DD format. This applies only to unencrypted APFS images; FileVault encryption must be disabled before acquiring the E01 image.
- Unencrypted macOS APFS images require no password, and the MACOS LOGIN tab is unavailable when configuring the logical extraction job.

Figure 179

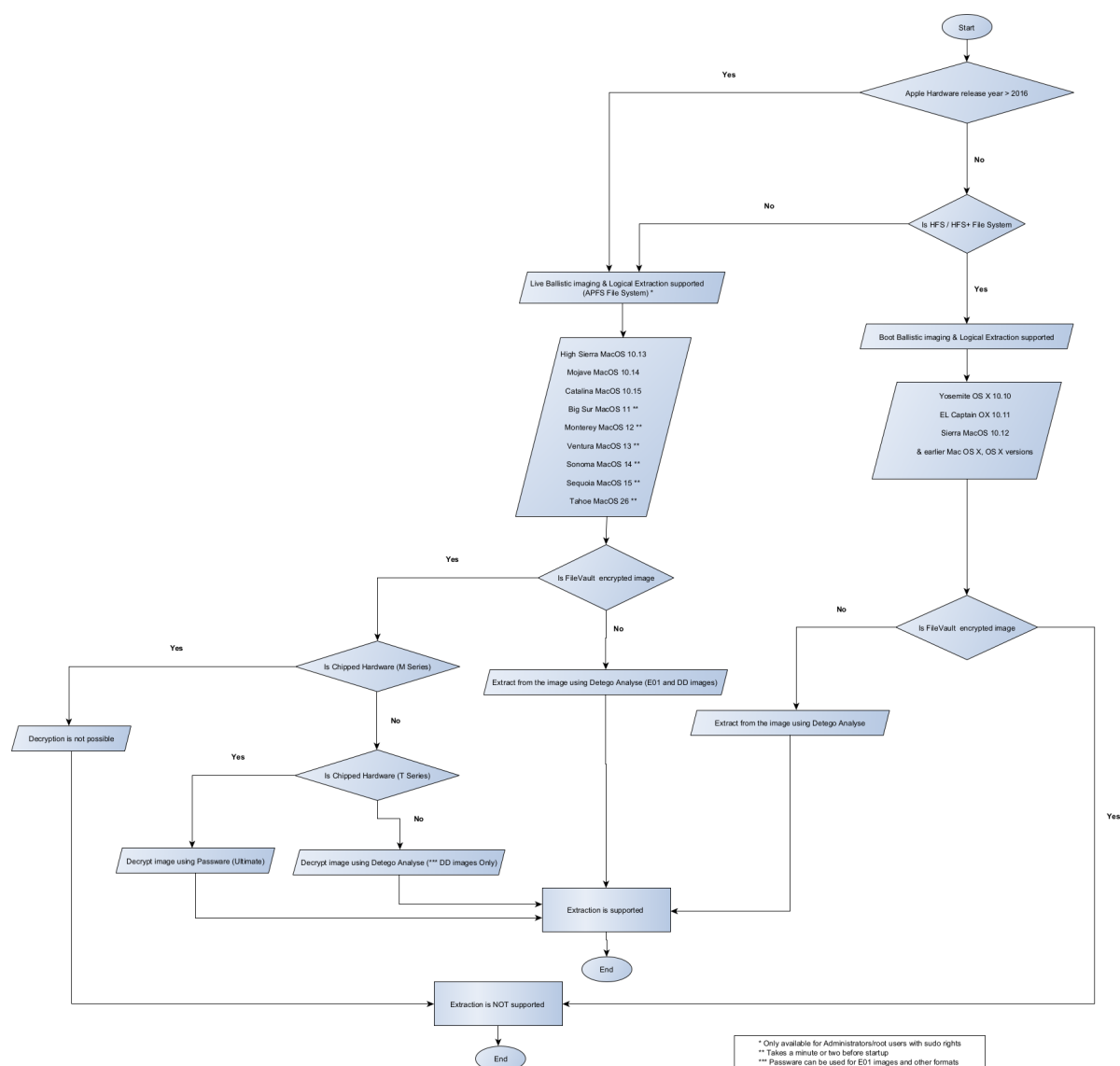


Figure 180

Detego Field 2026.1 or newer							
MacOS Name	Version Number	Release Year	File System	Live ¹		Boot	
				Ballistic	Logical	Ballistic	Logical
Tahoe ²	MacOS 26	2025	APFS	Yes ⁴ ; ⁵ ; ⁶ ; ⁷	Yes	Not Supported	
Sequoia ²	MacOS 15	2024					
Sonoma ²	MacOS 14	2023					
Ventura ²	MacOS 13	2022					
Monterey ²	MacOS 12	2021					
Big Sur ²	MacOS 11	2020					
Catalina	MacOS 10.15	2019					
Mojave	MacOS 10.14	2018					
High Sierra	MacOS 10.13	2017				Yes ⁴	No
Sierra	MacOS 10.12	2016	HFS	Not Supported		Yes ³	Yes
El Capitan	OS X 10.11	2015					
Yosemite	OS X 10.10	HFS					

¹ Only available for Administrators/root users with sudo rights.

² It may take a couple of minutes to start.

³ Supported unless there is a FileVault-encrypted image.

⁴ The ballistic image will be encrypted as an APFS filesystem for the entire physical drive.

⁵ If there is no FileVault-encrypted image, extract from the image using any 3rd party tool that supports APFS.

⁶ If the device has a T Series chip (not M Series), use Passware Ultimate to decrypt the image. If not, use any version of Passware to decrypt. (These are separate products and addons, please contact marketing@detegoglobal.com for more information).

⁷ If the device has an M Series chip, unfortunately, decryption and extraction are not possible.

LIVE

- Live extractions are only possible on APFS File Systems on hardware that was released after 2016.

- Live extractions are only available for Administrators or root users with sudo rights.
- On MacOS 11 (Big Sur) and newer, it may take a few minutes to start up.
- If the device has a FileVault-encrypted image, the following notes give details:
 - If the hardware has a T Series chip, you will need to decrypt using Passware Ultimate or another tool that can decrypt T Series-chipped MacOS.
 - If the hardware does not have a T Series chip, you can decrypt the image using any Passware version.
 - Chipped Hardware (M Series) cannot be decrypted currently; therefore, extraction is not possible.
- If the device does not have a FileVault-encrypted image, you can extract from the image using a third-party tool that supports APFS.

BOOT

- Boot is only supported on devices older than 2016 using an HFS File System.
 - Please be aware that a machine running MacOS Catalina and older should run in Boot OK. For example, if you have a Mac from 2017 that originally came with High Sierra or Mojave, and you upgrade to Catalina, it should boot okay.
- Detego Field for MacOS can't boot from a MacOS device if the hardware contains a T2 Chip introduced in 2018 with Mojave due to hardware encryption.

5.9. DETEGO FIELD CONFIG

Within the Detego Field stick, the 'Config' tool is used to configure extraction profiles for Detego Field.

- Once the user has inserted the Detego Field device, open the Detego Field folder and run the "Config" tool.
 - On Windows this is named Config.exe
 - On MacOS this is named Config_mac

- Once the tool starts you will see the below screen:

Figure 181

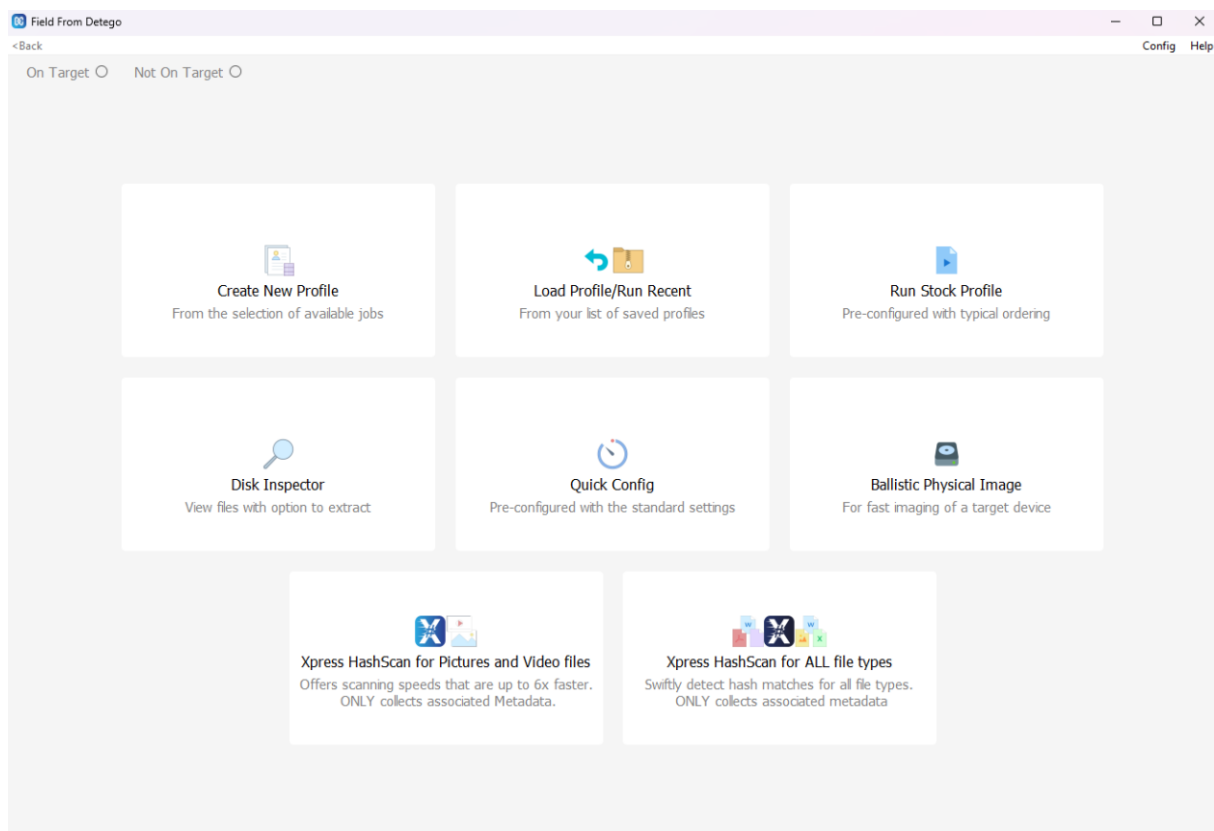
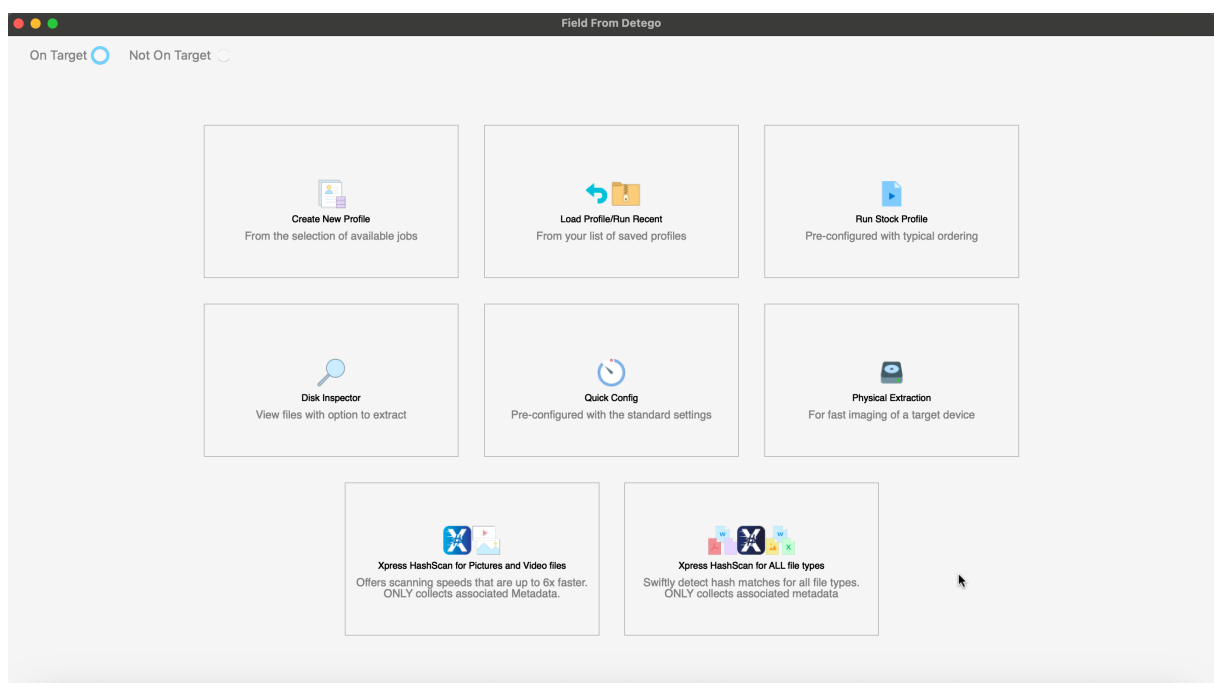


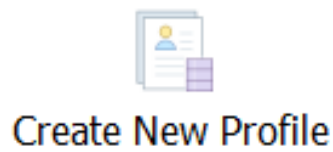
Figure 182



Below is a brief description of each available option in the Config tool and its function.

CREATE NEW PROFILE

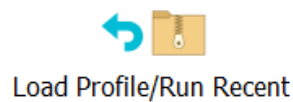
Figure 183



Create a new profile using the 'Profile Config.' This will allow you to configure all the parameters of a job and the order in which it runs.

LOAD PROFILE / RUN RECENT

Figure 184



Allows you to load a previously created profile to run or edit it further, or you can re-run the most recently run or edited profile. The user is also given the option to edit the profile before running it.

RUN STOCK PROFILE

Figure 185



Select a pre-built profile from a library of common extractions. You can run the profile or edit it and save it as a new profile.

DISK INSPECTOR

Figure 186



View files and folders on the target device you wish and extract any selected files.

QUICK CONFIG

Figure 187



Ideal for time-critical situations, this option opens a simplified version of the 'Profile Editor' with limited customisation options.

BALLISTIC PHYSICAL IMAGE

Figure 188

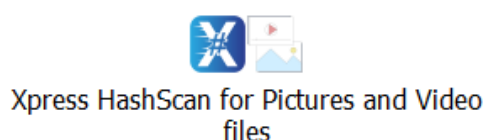


Run a Ballistic Imager acquisition of any drives connected to your target machine.

If you haven't purchased Detego Ballistic Imager, this will appear as 'Physical Extraction' instead for use in imaging drives without the Ballistic speed gains.

XPRESS HASHSCAN FOR PICTURES AND VIDEO FILES

Figure 189

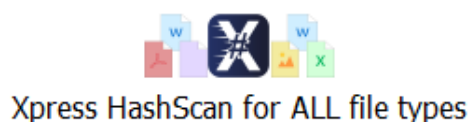


Run the **Xpress HashScan for Pictures and Video Files** option to scan the Picture and Video files faster and only check for hash matches for those media files without checking file headers, cloud files, or inside archive/links files.

No keyword matching or file type selection is permitted for this express scan mode. ONLY collects associated Metadata.

XPRESS HASHSCAN FOR ALL FILE TYPES

Figure 190



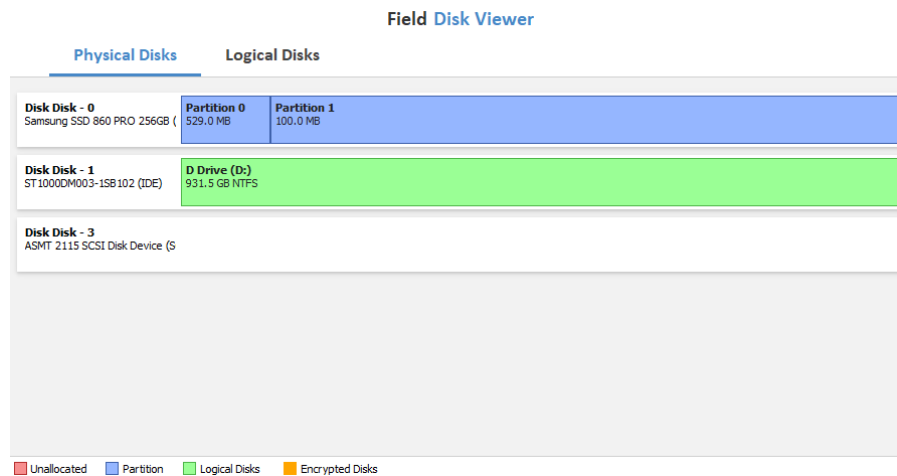
Run the **Xpress HashScan for ALL file types** option to scan all file types quickly and only check for hash matches for those media files without checking file headers, cloud files, or inside archive/links files.

No keyword matching or file type selection is permitted for this express scan mode. ONLY collects associated Metadata.

DISK VIEWER

If you wish to view the basic information of a Disk, navigate to Config (top right of the window), then select Disk Viewer from the dropdown menu. This will create an additional window displaying all Physical and Logical Disks.

Figure 191



If on MacOS, this menu can be found at the top of the screen in the MacOS menu bar.

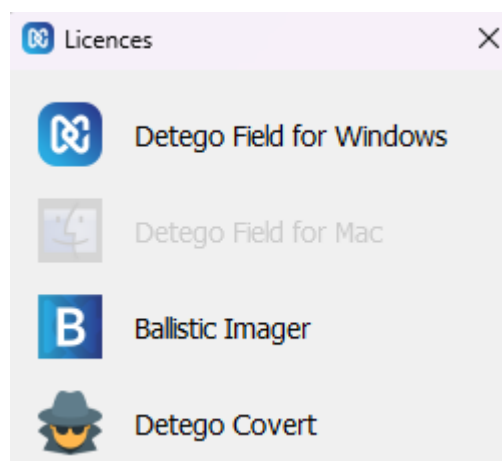
FIELD LICENSES

If you wish to view your License details for Detego Field, navigate to Config (top right of the window), then select Licenses from the dropdown menu. This will create an additional window displaying the licenses you Detego Field device holds.

This will include one or more of the following:

- Detego Field for Windows
- Detego Field for Mac
- Ballistic Imager
- Detego Covert

Figure 192



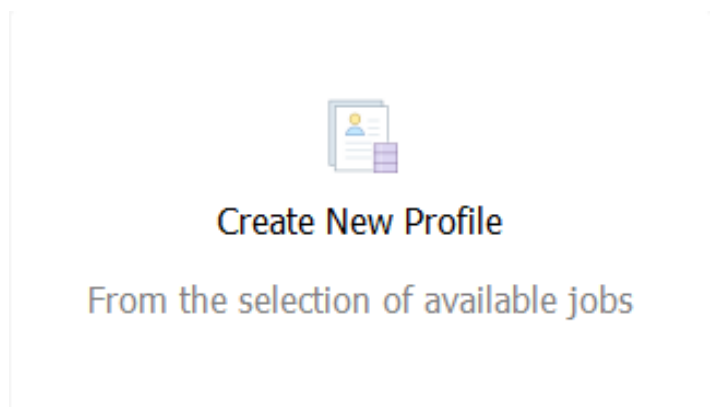
If on MacOS, this menu can be found at the top of the screen in the MacOS menu bar.

CREATE A NEW PROFILE

If you wish to customise your extraction type, select the 'Create New Profile' tile to view all available jobs.

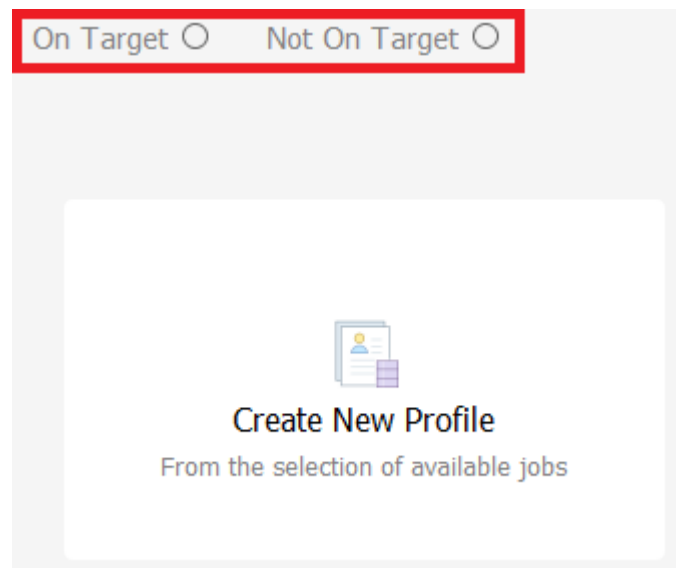
This will open the 'New Extraction' screen. From this screen, you can configure your extraction.

Figure 193



On Target / Not on Target

Figure 194



- **On Target** – Select this if you are the target machine. Disks and User Directories are configurable for On Target extractions.
- **Not on Target** – Select this if you are not on the target machine. Disks and User Directories are not configurable for Not on Target extractions. This is useful when creating profiles to be used on a number of different target devices.

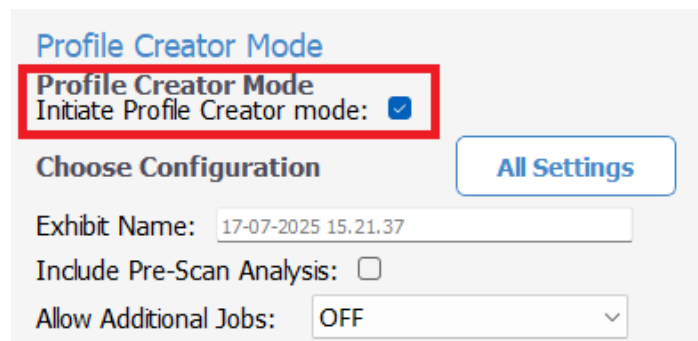
PROFILE CREATOR MODE

Profile Creator is a feature to prepare configuration files for Field jobs for less experienced or technical users. The function is to create a profile similar to the 'Run.exe/run_mac'; however, it will run a specific configuration based on your needs.

To create a profile, follow the below steps:

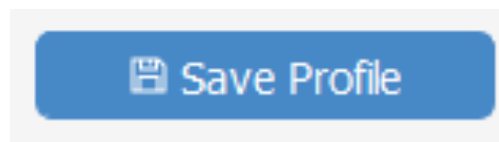
- Once in the “Create New Profile” section, select the 'Initiate Profile Creator mode' checkbox.
 - May not be applicable for MacOS.

Figure 195



- Selecting the checkbox will change the 'New Extraction' title to 'Profile Creator Mode' and grey out the buttons in the bottom right corner.
- Select any job you wish to configure, and when ready to save, select the 'Save Profile' button in the top right corner and rename as you wish.

Figure 196



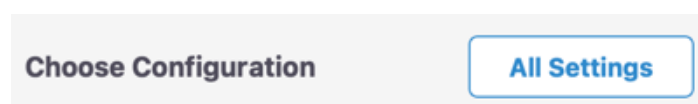
Once you have saved your profile to the stick, you will be able to load the profile using the 'Load Profile/Run Recent' tile.

You will also be able to import all profiles from your stick into Detego Analyse, allowing them to be licensed onto other Field devices. This removes the need to constantly create the same profiles repeatedly.

CONFIGURING ADDITIONAL SETTINGS

When creating a profile or extraction, you can select the 'All Settings' button to view and change any of the settings for the profile/extraction.

Figure 197



There are four tabs in the Additional Settings window. They are listed below:

MODE:

- User Mode – This allows you to select the type of user for the profile. These are either Standard or Covert. (Covert is only available if you have added to the licensed Detego Field device.)
- Copy Mode – This allows you to select the type of copy for the profile. These are either encrypted or Hash Only.
- **Windows Only** - You can change carving option here. Turning this option OFF will make the carving job quicker but at the costs of accuracy when identifying deleted file.

Figure 198

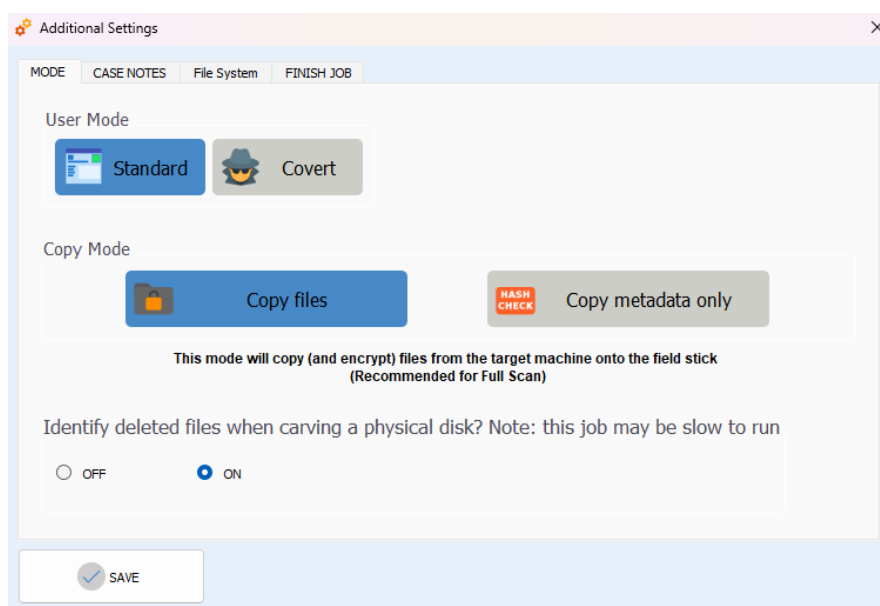
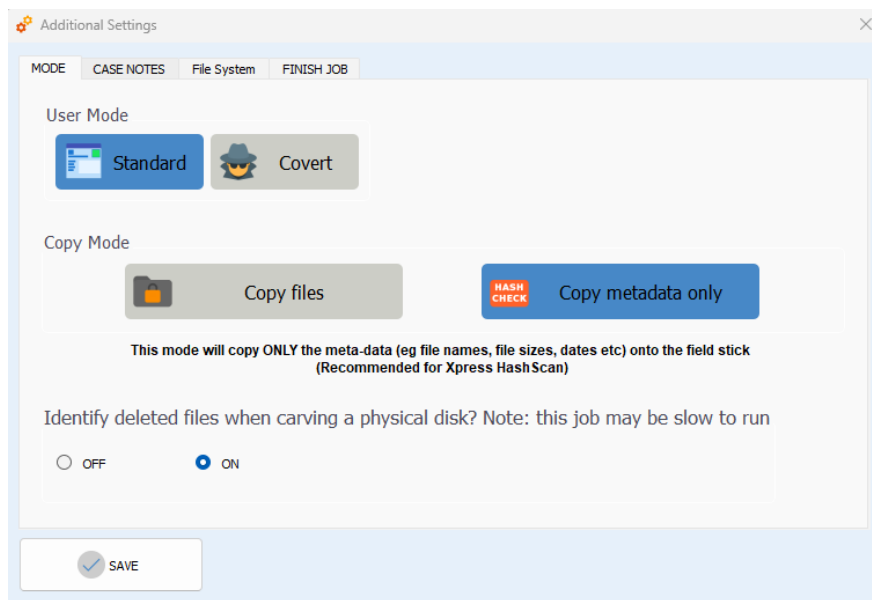


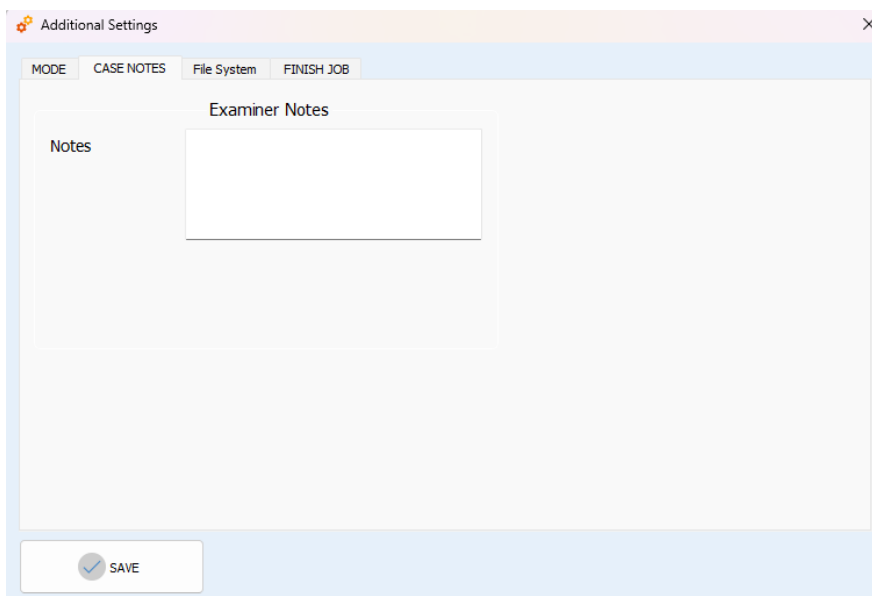
Figure 199



CASE NOTES:

NOTES/EXAMINER NOTES

Figure 200



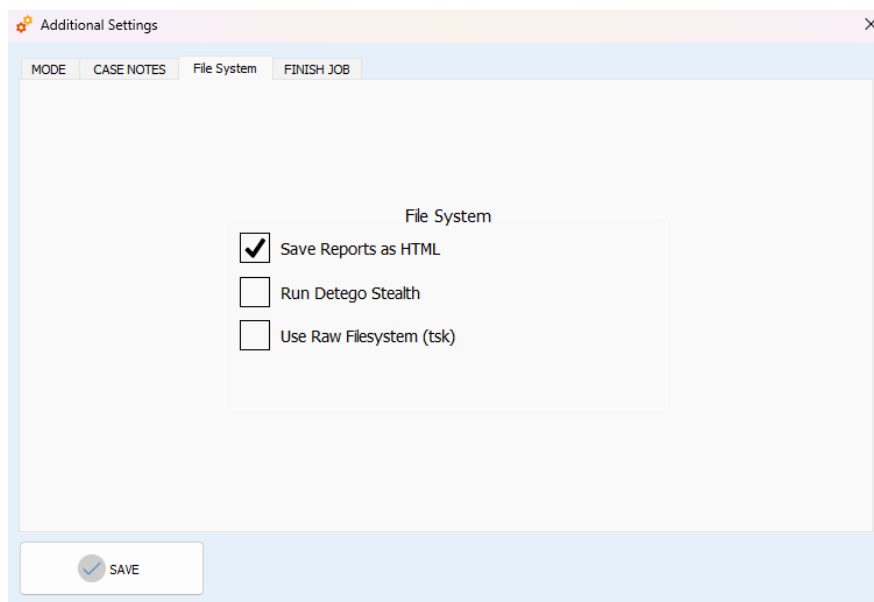
This section allows you to fill in any notes before you run the profile.

FILE SYSTEM:

- Save Reports as HTML

- Run Detego Stealth
- **Windows Only** - Use Raw Filesystem (tsk)

Figure 201

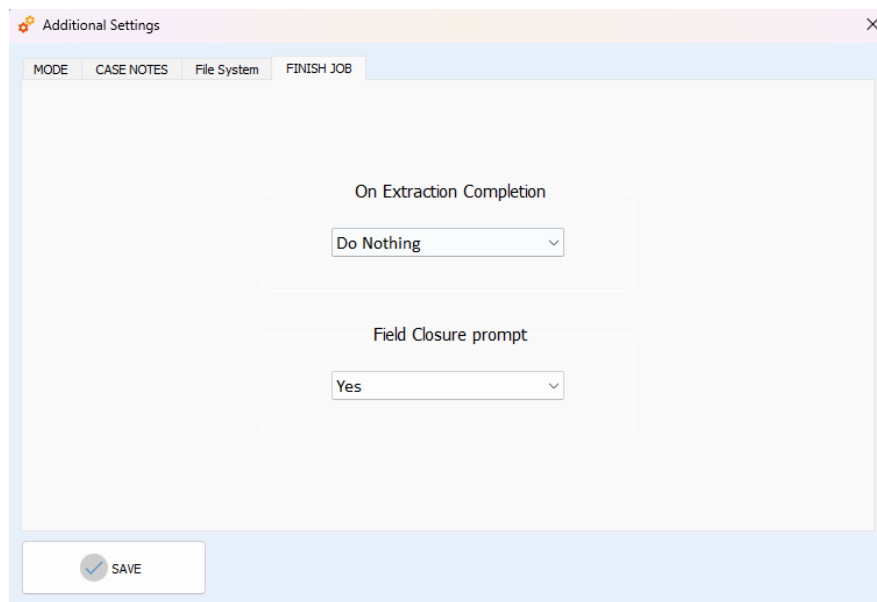


This section allows you to select various File System options.

FINISH JOB:

- **On Extraction Completion (Windows Only)**
 - The dropdown allows you to select the action that happens when a job is completed. These are Do Nothing, Close Detego, Logoff, and Shut Down.
- **Field Closure Prompt**
 - The dropdown allows you to select whether or not you are prompted when closing Detego Field.

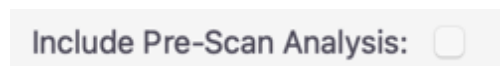
Figure 202



PRE-SCAN ANALYSIS

The Pre-Scan Analysis checkbox allows you to analyse the device/target drives. This will provide a breakdown of what type of files are on each disk, their capacity, the CPU speed and disk speed (the disk speed is usually dependent on the slowest disk on the system).

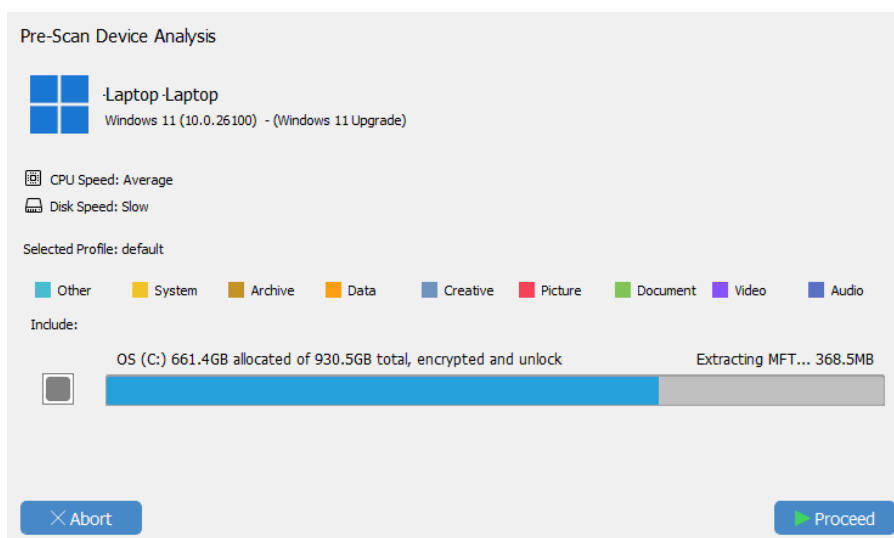
Figure 203



This feature can help determine a timeframe for the extraction process.

You can also abort the job if you don't wish to run the extraction. If you are happy with it, select 'Proceed'.

Figure 204



MEMORY EXTRACTION / BOOTCAMP MEMORY

The “Memory Extraction” job on Windows or the “Bootcamp Memory” job on MacOS targets volatile memory rather than long-term storage (the data an application stores while it’s in use and freed up once it’s closed).

It’s recommended that you extract memory first because it’s constantly changing, and any useful data may be lost the longer it’s left. Also, as Detego Field runs on the target machine, it takes up more memory the longer it is used, leaving less of the original data in the RAM.

Note: On average less than 1% of RAM is overwritten during Memory Extraction.

Figure 205

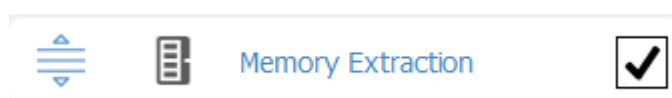
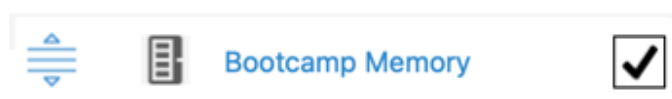


Figure 206



MEMORY EXTRACTION (WINDOWS):

Within the the Windows job, Memory Extraction, the following options are available:

Live System Memory:

- Extract RAM
 - This is the RAM (Random Access Memory) on a live machine. It stores all the data from running processes and will have leftovers from processes that have now been closed. Some of this data can hold useful forensic information, but it is lost the longer you leave it. If a machine is powered off, the data in the RAM is lost, so if a target machine is found switched on, it's often helpful to perform a memory extraction as soon as possible.

If you use the Boot Environment, you cannot extract the live RAM.

Offline System Memory:

When a computer shuts down, it leaves behind a few files to make booting up faster next time it's switched on.

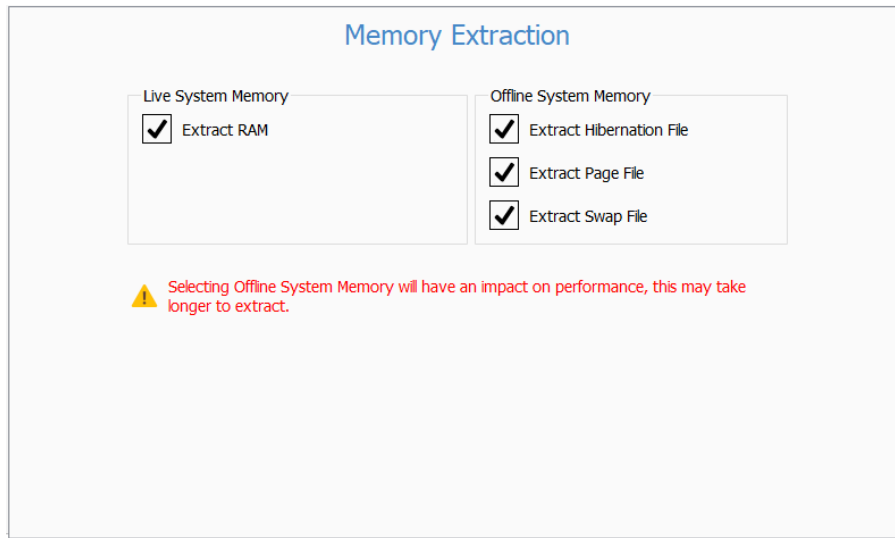
- Extract Hibernation File
- Extract Page File
- Extract Swap File

They're not quite as useful as RAM from a live machine, but can still hold useful forensic data. These files will be locked on a live machine, so you'll likely be unable to extract them.

However, these files will be extracted in the Boot Environment if present.

By default, all potential sources of memory are enabled. Detego Field will attempt to extract these files in Live mode, but unless you use the Raw Filesystem mode, the files will be locked, and permission will be denied.

Figure 207



The screenshot shows a dialog box titled "Memory Extraction". It contains two main sections: "Live System Memory" and "Offline System Memory". In the "Live System Memory" section, the option "Extract RAM" is checked. In the "Offline System Memory" section, the options "Extract Hibernation File", "Extract Page File", and "Extract Swap File" are all checked. Below these sections, a warning message with a yellow triangle icon states: "Selecting Offline System Memory will have an impact on performance, this may take longer to extract."

BOOTCAMP MEMORY (MACOS):

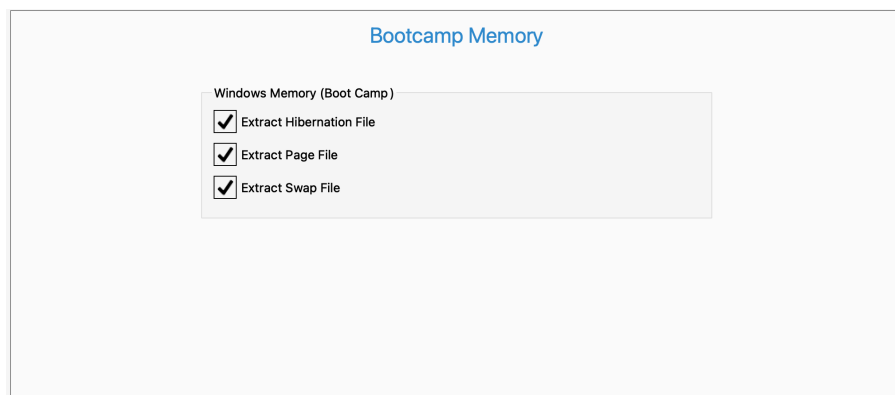
Within the the MacOS job, Bootcamp Memory, the following options are available:

Windows Memory (Boot Camp):

This is similar to the Windows job of Memory Extraction > Offline System Memory.

- Extract Hibernation File
- Extract Page File
- Extract Swap File

Figure 208



The screenshot shows a dialog box titled "Bootcamp Memory". It contains a section labeled "Windows Memory (Boot Camp)". Within this section, the options "Extract Hibernation File", "Extract Page File", and "Extract Swap File" are all checked.

DECRYPTION (BETA)

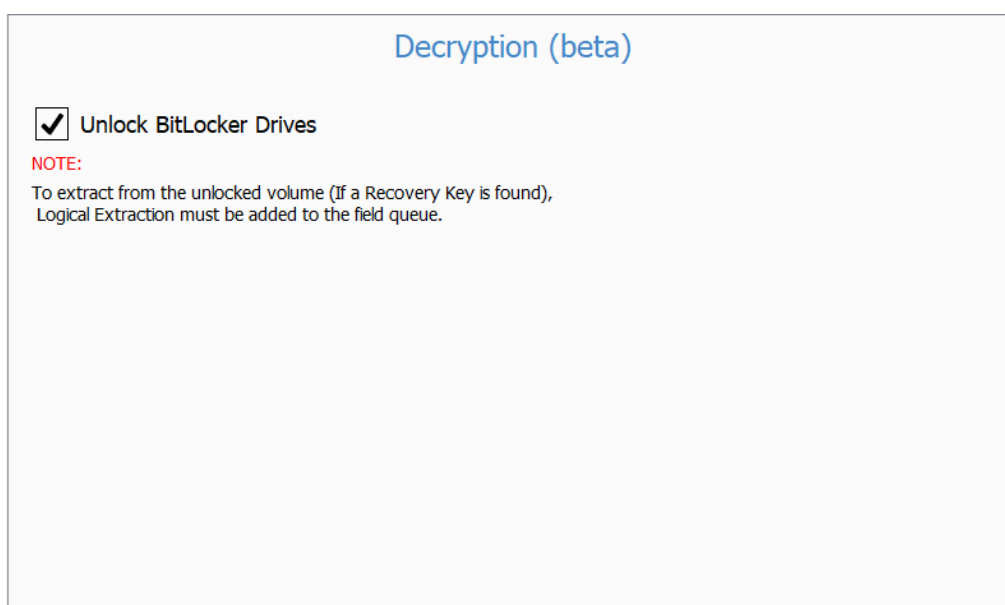
The Decryption (beta) job allows you to unlock a BitLocker encrypted drive if a Recovery Key is found.

Figure 209



Select the checkbox to enable this.

Figure 210



NOTE! To extract from the unlocked volume (If a Recovery Key is found), Logical Extraction **MUST** be added to the job queue in Detego Field.

SYSTEM INFORMATION

Detego Field can pull system information from all three major operating systems. The most comprehensive information from Windows can be collected live from the target machine or the Boot Environment.

This table details the information available on each operating system:

Figure 211

Information Available	Windows	Linux	MacOS
User Information	Boot**	Boot	Boot
Connected Networks*	Live & Boot	Boot	Boot
Installed Programs*	Live & Boot	Boot	Boot
OS Install Information	Live & Boot	Boot	Boot
USB History*	Live & Boot	N/A	Live & Boot
Run Commands*	Live & Boot	Boot	N/A
Recent Applications*	Live & Boot	N/A	N/A
Default Applications	Live & Boot	N/A	N/A
Recent Files	Live & Boot	N/A	N/A
Typed Paths*	Live & Boot	N/A	N/A
User Assist Data*	Live & Boot	N/A	N/A
Hardware	Live	N/A	Live

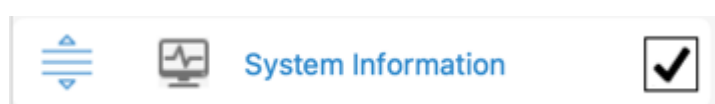
*This data can be keyword-matched based on the keyword lists set up during configuration.

** This data is also accessible from live Windows machines using the Raw Filesystem feature.

To configure a System Information job, follow the steps below:

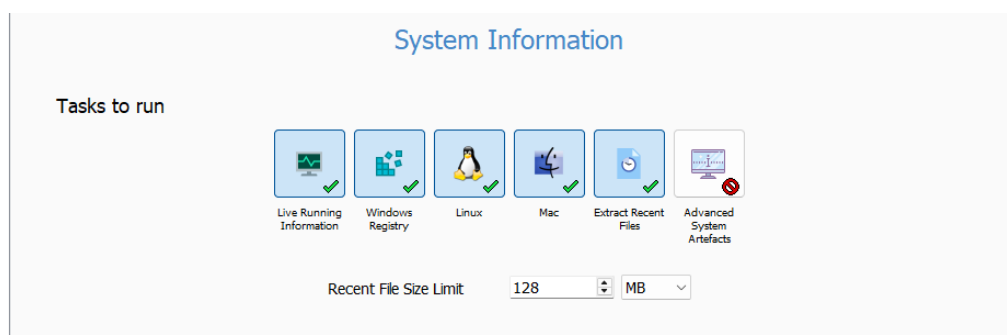
- Select the System Information checkbox in the Job Order list.

Figure 212



- Ensure you have selected each option you wish to extract during the job.

Figure 213



- The available options are below:
 - **Live Running Information:** This task extracts details from running applications, active network connections and disk partitions. If you're on a live machine, it will also look at the active hardware and network adapters.
 - **Windows Registry:** The registry stores most of its software settings, including those about itself. Here, you'll extract the list of installed applications, USB device history, recent file lists and more.
 - **Linux:** Linux doesn't store as much information as Windows, but numerous logs can be parsed to extract useful information, such as users and network connection history.
 - **Mac:** Although similar to Linux, OSX does have some extra information. For example, the software 'Finder' stores a list of attached media like USB devices.
 - **Extract Recent Files:** Extracts list of recent files for every user. These lists also contain details of files deleted, moved, or located on an external drive that's no longer connected. This task will extract recent files and the metadata of those removed recently.
 - **Advanced System Artefacts:** Advanced System Artefacts performs extractions of the data mentioned in the 'Description' column of the table.
 - If selecting this option, the following window will display:

Figure 214

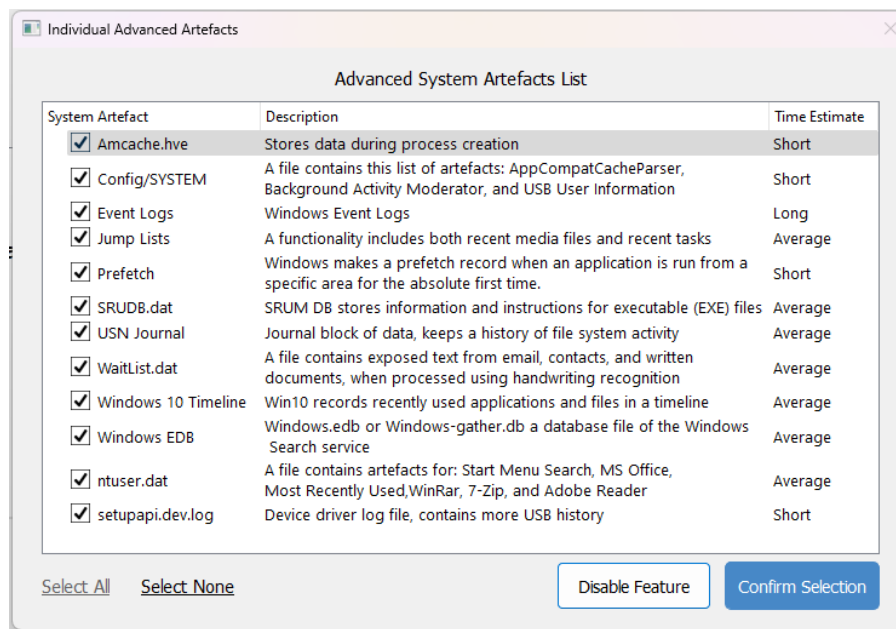
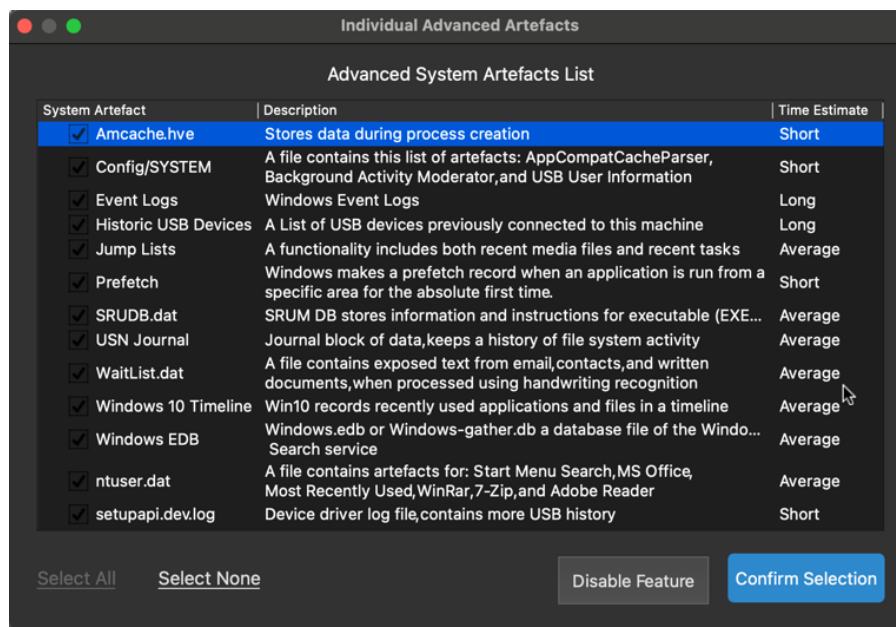


Figure 215



- Select the target directories you wish to extract System Information from:

Figure 216

[Select All](#) [Select None](#) [Apply to All Jobs](#)

	Username	OS	Home Directory
☒	Alex		C:\Users\Alex
☒	Alex.MCMS		C:\Users\Alex.MCMS
☒	Public		C:\Users\Public

Figure 217

[Select All](#) [Select None](#) [Apply to All Jobs](#)

	Username	OS	Home Directory
☒	macbookpro1		/Users/macbookpro1

- If you wish to run Keyword Matching on the System Information job, select the Keyword Matching checkbox and select which Keyword Lists you wish to match against.

Figure 218

☒ Keyword Matching ...

Figure 219

Keyword Manager

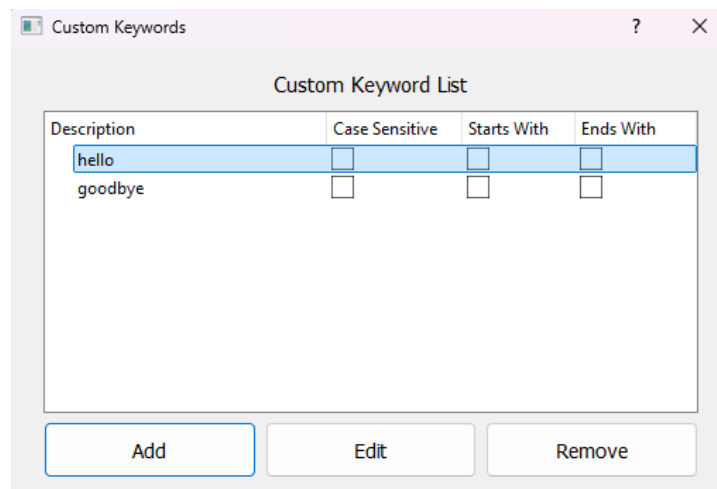
The Keyword Manager lets you turn on/off your keyword lists for this particular profile. Keyword Matching is done in 'System Information', 'Internet Artefacts', 'File Carve', and 'Logical' jobs.

☒ ▼

- ☒ [PREINSTALLED] Borders (47 Keywords)
- ☒ [PREINSTALLED] Cloud Apps (21 Keywords)
- ☒ [PREINSTALLED] Cryptocurrency (78 Keywords)
- ☒ [PREINSTALLED] Encryption (70 Keywords)
- ☒ [PREINSTALLED] IED Precursor (89 Keywords)
- ☒ [PREINSTALLED] P2P Apps (28 Keywords)

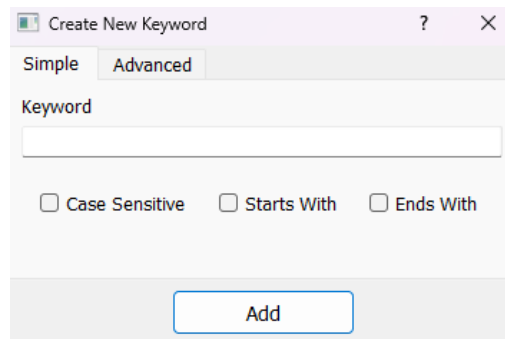
- If you would like to add, remove, or edit your custom Keywords, select the “Edit Custom Keywords”.
- Once you have selected this, the below window will display:

Figure 220



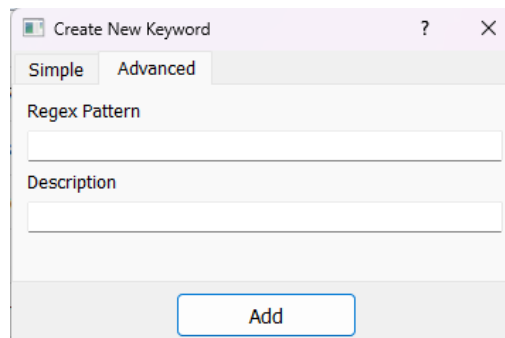
- Select Add to add a new Keyword. This will allow you to choose the following options:
 - **Simple Tab:**
 - **Keyword** - Type out your keyword.
 - **Case Sensitive** - Check this if you wish they keyword to be case sensitive.
 - **Starts With** - Allows Keyword Matching with words that have this keyword at the start.
 - **Ends With** - Allows Keyword Matching with words that have this keyword at the end.
 - **Advanced Tab:**
 - **Regex Pattern** - Input your Regex pattern.
 - **Description** - Describe the Regex pattern.

Figure 221



The 'Create New Keyword' dialog box is shown with the 'Simple' tab selected. It features a text input field for a keyword, three unchecked checkboxes labeled 'Case Sensitive', 'Starts With', and 'Ends With', and an 'Add' button at the bottom.

Figure 222



The 'Create New Keyword' dialog box is shown with the 'Advanced' tab selected. It features a text input field for a regex pattern, a text input field for a description, and an 'Add' button at the bottom.

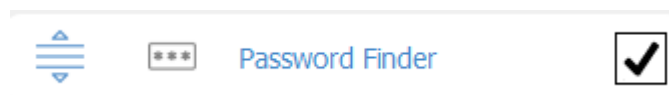
- Once you are happy with your selection, select the “Confirm” button to save your selection for this job.

PASSWORD FINDER

The 'Password Finder' feature can extract credentials (usernames and passwords) from various files left behind by popular software packages.

Although most software packages encrypt passwords before storing them on the disk, Windows will decrypt them for you if logged in, meaning this job is most effective on a live Windows machine. If you cannot log in as the user, the relevant files can still be extracted and brute-forced once imported into Detego Analyse.

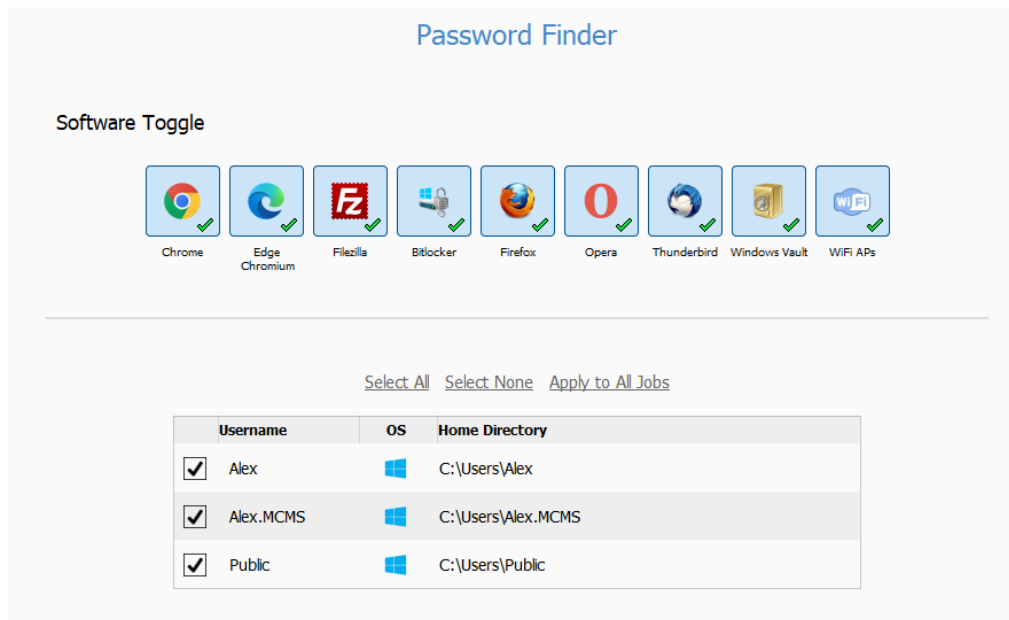
Figure 223



- Select the software package you would like to extract Passwords from (in the Software Toggle section).

- Select the Directory/Directories you wish to extract the Passwords from (the section below Software Toggle).

Figure 224



You can still retrieve unencrypted data from the various software packages even without logging in as a Windows user. The table below details what you can typically acquire:

Figure 225

Software Package	Logged in	Not Logged in
Google Chrome	Uenames Passwords	Uenames Encrypted Passwords
Edge Chromium	Uenames Passwords	Uenames Encrypted Passwords
FileZilla	Uenames Passwords	Uenames Passwords
Bitlocker	Recovery Keys	N/A
Firefox	Uenames* Passwords*	Uenames* Passwords*
Opera	Uenames Passwords	Uenames Encrypted Passwords
Thunderbird	Uenames* Passwords*	Uenames* Passwords*
Windows Vault	Uenames Passwords	N/A
WiFi APS	Uenames Passwords	Uenames Encrypted Passwords

*Mozilla encrypts usernames and passwords but leaves the encryption key on the disk. This encryption key doesn't have a password; however, the data cannot be decrypted by Detego Field if a user changes the default settings.

Once detected, these credentials are compiled into a report listing the most commonly used, including those for social media websites such as Facebook and Twitter. It also identifies duplicated passwords.

Click on 'Password Finder' to display the advanced settings; all options are enabled by default.

Use the 'Software Toggle' to choose which supported software packages to search.

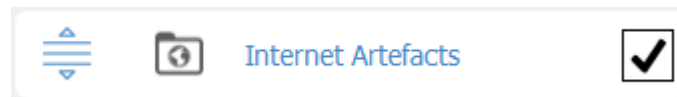
If you're working in 'On Target' mode, you can pick individual users to target by unticking the 'Search all available users' Field and choosing from the list.

INTERNET ARTEFACTS

Modern web browsers and chat programs use a variety of databases to keep track of a user's data so it can be retrieved quickly without waiting for an online server to respond. Data stored in the cloud, such as browser history and bookmarks, are downloaded locally for quicker access.

These files left on the system (artefacts) can reveal much about the machine's user, including the websites visited, search history, downloads, and, in some cases, even a complete log of all the chats they've participated in.

Figure 226



BROWSER TOGGLE:

- Within the “Internet Artefacts” job, toggle on/off the Applications you would like to extract Internet Artefacts from (by default, all options are enabled).

Figure 227



Figure 228



- The following table shows the available applications for Windows and/or MacOS.

Figure 229

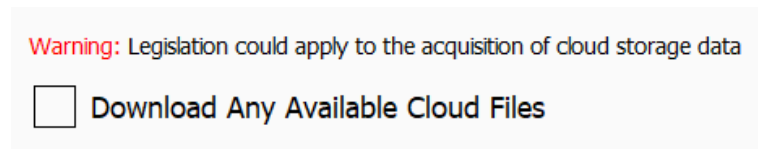
Icon	Name	Detego Field for Windows	Detego Field for MacOS
	Signal	Yes	Yes
	WhatsApp	Yes	Yes
	Brave	Yes	Yes
	Chrome	Yes	Yes
	Epic Privacy Browser	Yes	Yes
	Firefox	Yes	Yes
	Internet Explorer 9	Yes	Yes
	IE10+ (Edge-Legacy)	Yes	Yes
	Edge Chromium	Yes	Yes
	Safari	Yes	Yes
	Opera	Yes	Yes
	Vivaldi	Yes	Yes
	Skype	Yes	Yes
	Outlook	Yes	No
	Thunderbird	Yes	No

DOWNLOAD CLOUD FILES:

- If you wish to download any available cloud files from the above applications, please check the box.

- **WARNING!** Local legislation may apply to the acquisition of cloud storage data so please confirm what this entails for you before selecting this option.

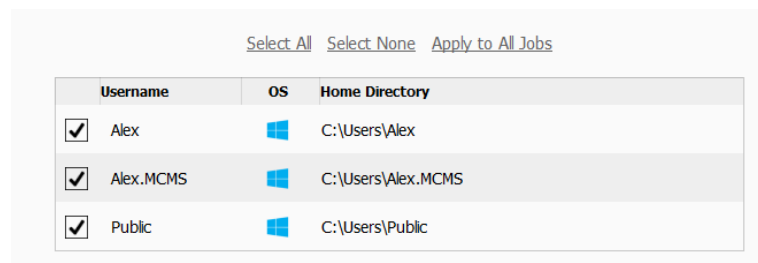
Figure 230



DIRECTORIES SELECTION:

- Select the directories you wish to extract Internet Artefacts from.

Figure 231



KEYWORD MATCHING:

- If you wish to run Keyword Matching on the Internet Artefacts job, select the Keyword Matching checkbox and select which Keyword Lists you wish to match against.

Figure 232

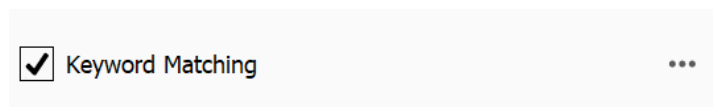
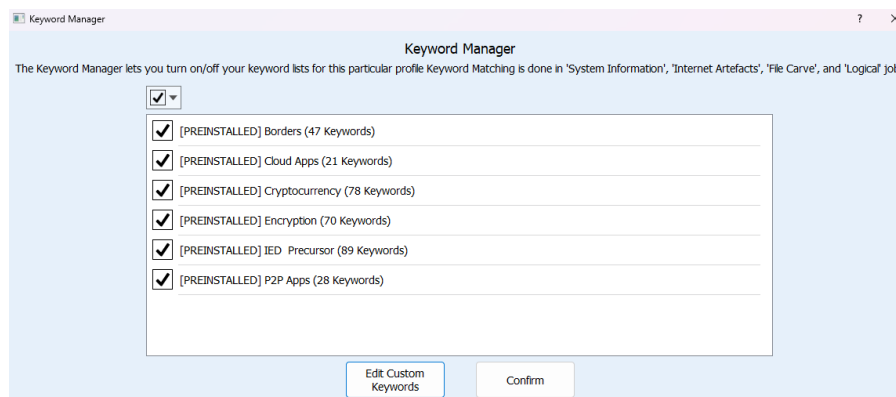
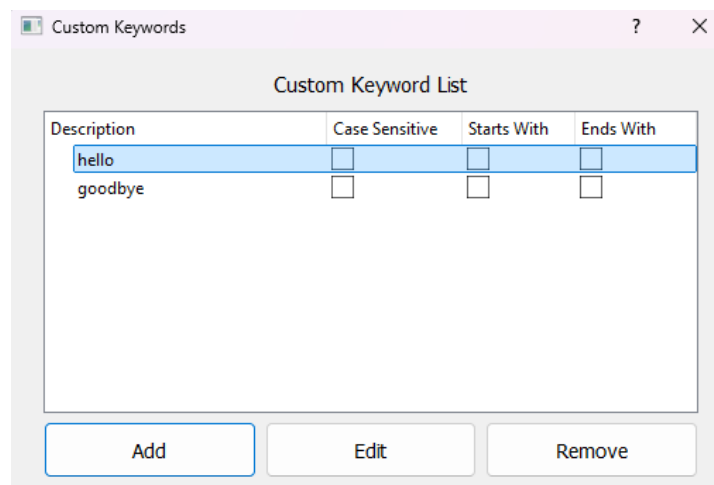


Figure 233



- If you would like to add, remove, or edit your custom Keywords, select the “Edit Custom Keywords”.
- Once you have selected this, the below window will display:

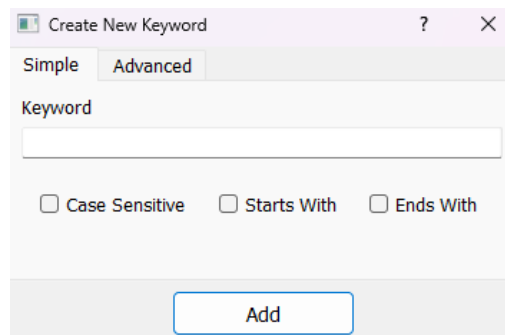
Figure 234



- Select Add to add a new Keyword. This will allow you to choose the following options:
 - **Simple Tab:**
 - **Keyword** - Type out your keyword.
 - **Case Sensitive** - Check this if you wish they keyword to be case sensitive.
 - **Starts With** - Allows Keyword Matching with words that have this keyword at the start.

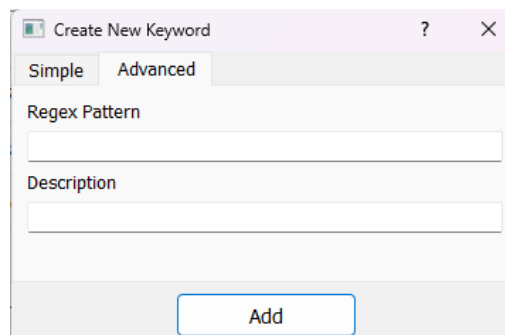
- **Ends With** - Allows Keyword Matching with words that have this keyword at the end.
- **Advanced Tab:**
 - **Regex Pattern** - Input your Regex pattern.
 - **Description** - Describe the Regex pattern.

Figure 235



The screenshot shows a dialog box titled "Create New Keyword" with a close button (X) and a help button (?). It has two tabs: "Simple" (selected) and "Advanced". Under the "Simple" tab, there is a text input field labeled "Keyword". Below the input field are three checkboxes: "Case Sensitive", "Starts With", and "Ends With". At the bottom of the dialog is an "Add" button.

Figure 236



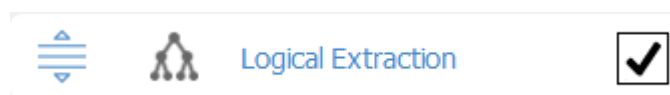
The screenshot shows the same "Create New Keyword" dialog box, but with the "Advanced" tab selected. Under the "Advanced" tab, there are two text input fields: "Regex Pattern" and "Description". At the bottom of the dialog is an "Add" button.

- Once you are happy with your selection, select the "Confirm" button to save your selection for this job.

LOGICAL EXTRACTION

The file system and directories on a computer make up its logical data. This is how data appears when using an operating system like Windows or MacOS.

Figure 237



When selecting Logical Extraction you will have a choice of how you would like to configure your extraction.

- **Basic Selection** - A straight forward option to grab as much data as possible.
- **Custom (Advanced)** - This selection lets you be more specific about the file/folder paths you wish to extract or ignore. This is more of an advanced feature if you want to extract from specific locations on the machine.

BASIC SELECTION

If you have selected the Basic Selection radio button, you can choose to extract User Directories and/or Entire Disks.

- Simply select the User Directories and/or Entire Disks you wish to extract.
- If you wish to search non-checked users during a full system scan, select the checkbox under the User Directories section.

NOTE! The list of disks displays all physical drives connected to the target device. If you have Ballistic Collectors connected, they will not appear in this list.

Figure 238

Logical Extraction

Extraction Locations

☒ Basic Selection ☐ Custom (Advanced)

☒ User Directories

Select All Select None Apply to All Jobs

Username	OS	Home Directory
☒ Alex	Windows	C:\Users\Alex
☒ Alex.MCHS	Windows	C:\Users\Alex.MCHS
☒ Public	Windows	C:\Users\Public

☐ Search non-checked users during full system scan

☒ Entire Disk

Mountpoint	Label	Location	Size
☒ C:\	OS	INTERNAL	267.6GB (Free 205.5GB)

A Detego logo will appear next to drives that either have Detego Analyse installed or are recognised as a Field Device. The right-click option is available to hide unavailable drives. (This includes Detego Field/Ballistic devices).

CUSTOM (ADVANCED)

If you are an advanced user or wish to extract from specific locations on the target device, you can input your own custom Extraction Paths or Ignore Paths.

- Simply select the “Custom Paths” toggle to enable Custom Paths.
- Within Extraction Paths/Ignore Paths, enter the custom path you wish to add and then select “Add”
- You can remove any Extraction Paths/Ignore Paths in this section using the “Remove” button next to each path.

Figure 239

The screenshot displays the 'Logical Extraction' configuration window. Under 'Extraction Locations', the 'Custom (Advanced)' radio button is selected. The 'Custom paths' checkbox is checked. A blue informational message states: 'To search only custom paths, please ensure you remove existing generic extraction paths.' Below this, the 'Extraction Paths' section contains two entries: '<VOL>' and '<USERS>', each labeled as a 'Generic path' with a corresponding 'Remove' button. An 'Extract Matched Files' section features a text input field labeled 'Enter custom path' and an 'Add' button. The 'Ignore Paths' section is currently empty, with a text input field labeled 'Ignore path: Enter custom path' and an 'Add' button at the bottom.

HASH MATCHING

Hash Matching allows you to hash match the data you are extracting using your hashlists created from Detego Analyse.

- Select the checkbox next to Hash Matching in order to enable hash matching. This will open up the following section:

Figure 240

☒ Hash Matching

☐ Ignore Safe Hash Files (e.g. NSRL)

Scan Options

☒ Full Scan Mode
Includes checking of headers, cloud files, inside archive files, extensions etc. Allows keyword matching, file type selection and other parameters

☐ Xpress HashScan for Pictures and Video files
Offers scanning speeds that are up to 6x faster. ONLY collects associated Metadata. No header checking and No scanning inside archive files.

☐ Check files without extensions **Note:** Tick this box to additionally scan files that do NOT have an extension. This will add time to the scan.

☐ Xpress HashScan for ALL file types
Swiftly detect hash matches for all file types. ONLY collects associated Metadata. No header checking and No scanning inside archive files.

Only Check files above: 0 Bytes

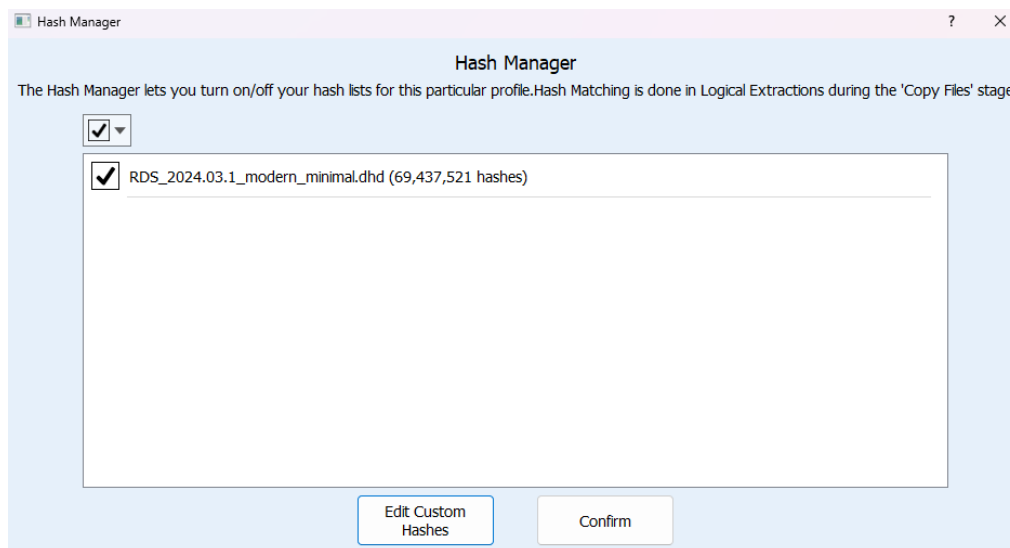
From here you can the following options:

- **Ignore Safe Hash Files (e.g. NSRL)**
 - This will ignore any safe hashlists you have added e.g. NSRL. This means the extraction will not extract known safe hash files.
- **Full Scan Mode**
 - This runs a full scan including checking of headers, cloud files, inside archive files, extensions etc. and allows keyword matching and other parameters.
- **Xpress HashScan for Pictures and Video files**
 - This scan mode offers scanning speeds that are up to 6x faster. It ONLY collects associated Metadata and does not perform any header checking or scanning inside archive files.
 - The checkbox under this option allows you to enable “Check files without extensions” which will scan files that do not have an extension, adding time to the scan.
- **Xpress HashScan for All file types**
 - This scan mode detects hash matches for all file types. It ONLY collects associated Metadata and does not perform any header checking or scanning inside archive files.

If you have selected either of the Xpress HashScan options, you can also specify a filesize of the scans to check files for (default is 0 Bytes).

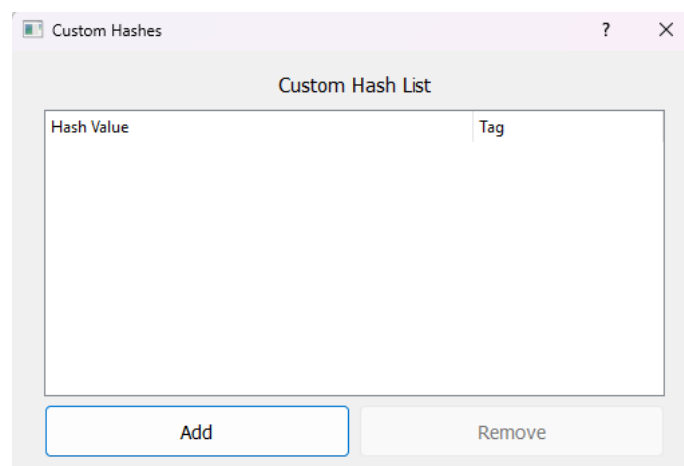
- Once you have selected your Scan mode, select the three dots menu on the right of Hash Matching option to open the Hash Manager window:

Figure 241



- Simply select any hashlist you wish to run hash matching against.
- If you wish to edit your custom hashes, select the "Edit Custom Hashes" button. This will open the below window where you can add your custom hash:

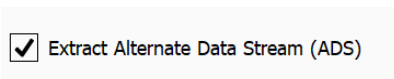
Figure 242



EXTRACT ALTERNATE DATA STREAM (ADS)

Selecting this will extract an Alternate Data Stream (ADS), mostly used to hide data from the user underneath the NTFS file system and store simple text strings.

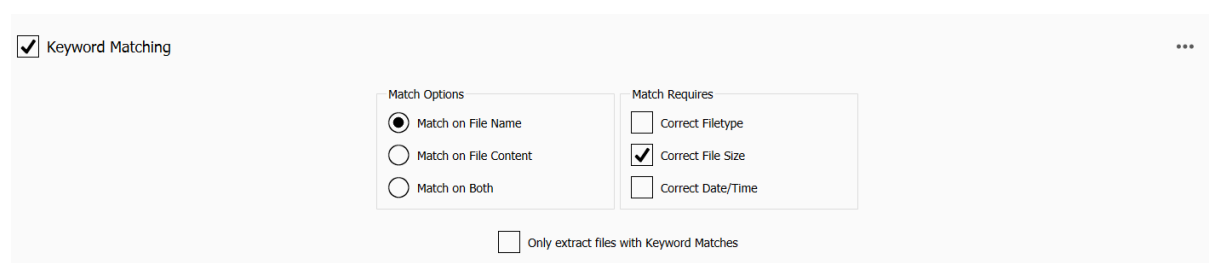
Figure 243



KEYWORD MATCHING

- If you wish to run Keyword Matching on the Logical Extraction, select the Keyword Matching checkbox to enable keyword matching.

Figure 244



Match Options:

Match options allows you to specify what Keyword Matches will match to.

- Match on File Name - This will match all the file name only and is the quickest method.
- Match on File Content - This will match on the file content only and has a time overhead.
- Match on Both - This will match on both the file name and file content and has a greater time overhead.

Match Requires:

These options allow you to specify what the requirements need to be met in order to keyword match.

- Correct Filetype - Checking this will enable correct filetype requirements and will only match with the correct filetype. Uses the File Type constraints in the Logical Extraction job.

- Correct File Size - Checking this will enable correct file size requirements and will only match with the correct file size. Uses the File Size constraints in the Logical Extraction job.
- Correct Date/Time - Checking this will enable correct file size requirements and will only match with the correct date/time. Uses the Date/Time constraints in the Logical Extraction job.

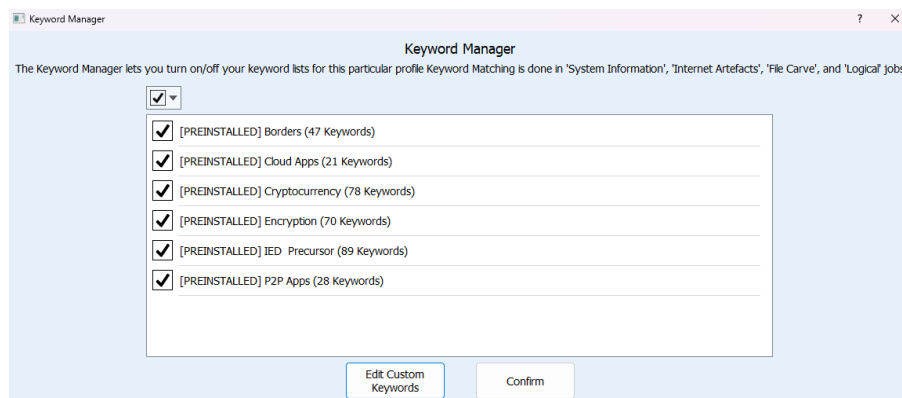
Only Extract Files with Keyword Matches:

- Selecting the “Only extract files with Keyword Matches” checkbox below the Match Options and Match Requirements sections will only extract Keyword Matched files.

Keyword Manager:

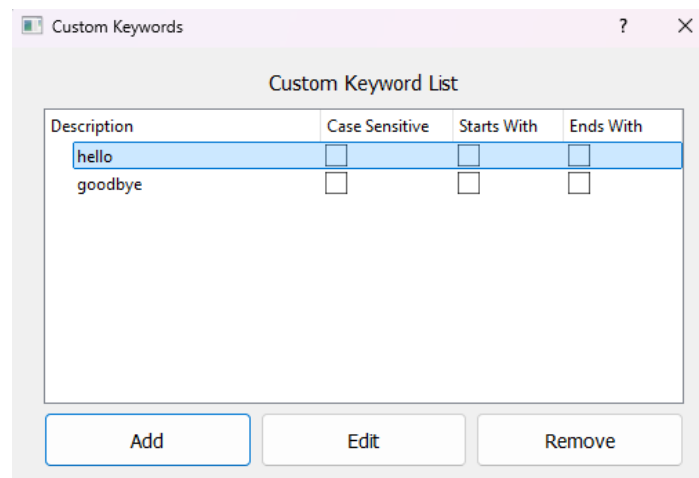
- If you would like to manage your keyword lists and custom keywords, select the three dot menu “...” to the right of the Keyword Matching option. This will open the below window.

Figure 245



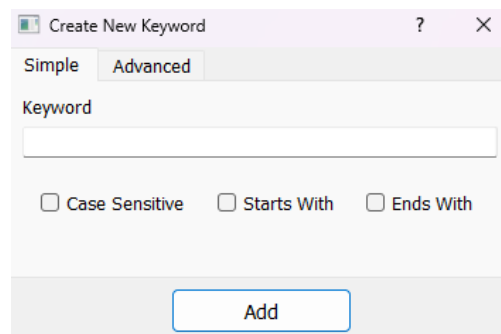
- If you would like to add, remove, or edit your custom Keywords, select the “Edit Custom Keywords”.
- Once you have selected this, the below window will display:

Figure 246



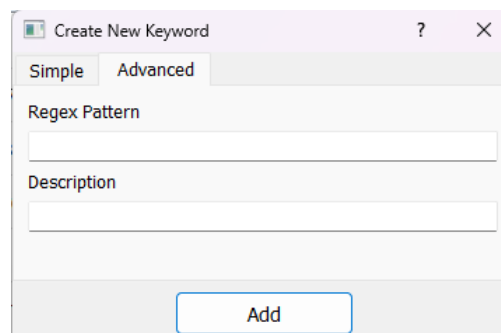
- Select Add to add a new Keyword. This will allow you to choose the following options:
 - **Simple Tab:**
 - **Keyword** - Type out your keyword.
 - **Case Sensitive** - Check this if you wish they keyword to be case sensitive.
 - **Starts With** - Allows Keyword Matching with words that have this keyword at the start.
 - **Ends With** - Allows Keyword Matching with words that have this keyword at the end.
 - **Advanced Tab:**
 - **Regex Pattern** - Input your Regex pattern.
 - **Description** - Describe the Regex pattern.

Figure 247



The dialog box titled "Create New Keyword" has two tabs: "Simple" and "Advanced". The "Simple" tab is selected. It contains a text input field labeled "Keyword". Below the input field are three checkboxes: "Case Sensitive", "Starts With", and "Ends With". At the bottom right is an "Add" button.

Figure 248



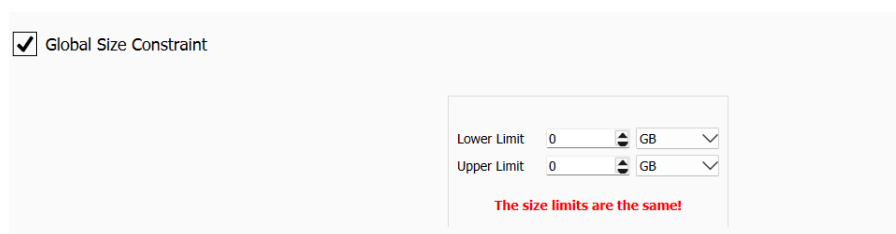
The dialog box titled "Create New Keyword" has two tabs: "Simple" and "Advanced". The "Advanced" tab is selected. It contains a text input field labeled "Regex Pattern" and another text input field labeled "Description". At the bottom right is an "Add" button.

- Once you are happy with your selection, select the “Confirm” button to save your selection for this job.

GLOBAL SIZE CONSTRAINT

- Selecting the “Global Size Constraint” checkbox allows you to specify lower and upper size limits for files.

Figure 249



The "Global Size Constraint" section is shown with the checkbox checked. Below it are two rows of input fields: "Lower Limit" and "Upper Limit". Each row has a numeric input field set to "0", a unit selector dropdown set to "GB", and a confirmation dropdown set to "v". Below these fields is a red text message: "The size limits are the same!"

EXTRACT ALL FILES

- If you wish to extract all files, regardless of filetype, then select the “Extract All File Types” checkbox.

Figure 250

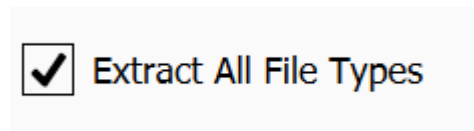
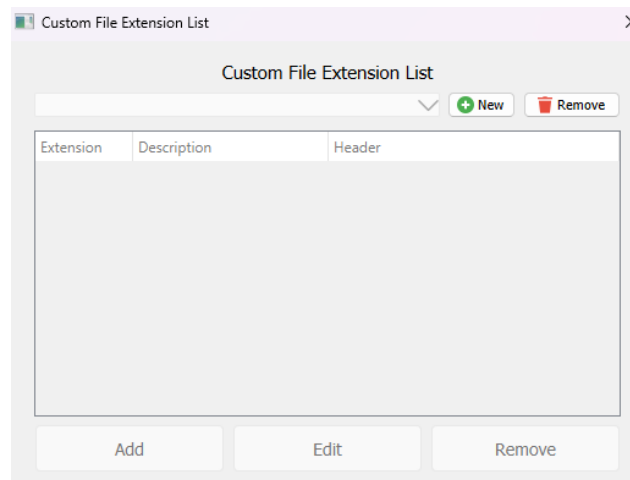


Figure 251

A screenshot of a software settings window titled 'Extract All File Types'. At the top, there are three checkboxes: 'Extract All File Types' (unchecked), 'Check File Headers' (unchecked), and 'Exclude 7Zip Unzipping' (unchecked). Below these is a table with five columns: 'File Type', 'Global Size Constraint', 'Custom Lower Limit', 'Custom Upper Limit', and 'Extension'. The table lists six file types: Picture, Document, Video, Audio, Email, and Camera. 'Picture' and 'Document' are checked, while the others are unchecked. Each row has a 'Global Size Constraint' dropdown (set to 'Global Size Constraint'), 'Custom Lower Limit' and 'Custom Upper Limit' dropdowns (both set to '0 Bytes'), and an 'Extension' dropdown. The 'Extension' dropdown for 'Picture' shows '170/170 selected' and for 'Document' shows '138/138 selected'. At the bottom right, there are two buttons: '+ Add Custom' and 'More Types'.

- If this is unchecked, you can manually choose which file types will be extracted as well as the below:
 - **Check File Headers** - Selecting this checkbox will enable checking of file headers (can increase time overhead).
 - **Exclude 7Zip Unzipping** - Selecting this checkbox will exclude 7Zip Unzipping. Currently 7Zip unzipping has a small time overhead and this will skip that. .7z archive files will still be extracted unless specifically excluded.
 - **Global Size Constraint** - You can select this from Global Size Constraint to Custom which then allows you to specify lower and upper size limits per file type.
 - **Extension** - This allows you select extensions you wish you enable/disable for extraction.
 - **More Type** - This button shows more File types.
 - **Add Custom** - If you wish to add custom file extensions, select the "Add Custom" button in the bottom right corner of the Extract All File Types section.

Figure 252



Please note that Legacy Field supports limited file extensions; using the Analytical job in Detego Media Acquisition will provide more results. Supported extensions are listed below:

Figure 253

extension_id	extension	category
83	.rar	Archive
145	.wma	Audio
404	.sqlite	Database
712	.bmp	Picture
745	.gif	Picture
770	.jpg	Picture
799	.png	Picture
807	.psd	Picture
842	.tif	Picture
843	.tiff	Picture
1011	.flv	Video
1121	.lha	Archive
1122	.tar.bz2	Archive
1123	.ipd	Database
1124	.3gpp	Video
1125	.wpl	Video
1126	.qel	Document
1127	.enl	Document
1128	.cpi	Document
1129	.cpi	Document
1130	.wb3	Document
1131	.cfg	System
1132	.suo	System
1133	.spvchain	Cryptography

- **More Types** – This button expands the section and shows all available file types. All main file types are: Picture, Document, Video, Audio, Email, Camera, Archive, 3D, Code, Cryptography, Data, Database, Disk Image, Drone, E-Book, Executable, Geographical and System.

DATE AND TIME CONSTRAINTS

- If you wish to enable date and time constraints, select the “Date and Time Constraints” checkbox. This allows you to specify a date/time range in either of the following methods:
 - Relative Time - This is the best option if the target device’s time is unknown.
 - Absolute Time - This goes back from the time on the target device’s clock.

Figure 254

☒ Date and Time Constraints

☒ Relative Time

From: 4 days ago
To: 2 hours ago
Range: 3 days 22 hours

☐ Absolute Time

From: 05 Mar 2019 10:00:00
To: 04 Mar 2020 10:00:00
Range: 1 year

CLOUD FILE ACQUISITION

- If you wish to download any available cloud files, select the “Download Any Available Cloud Files” checkbox.
 - **WARNING!** Please be aware that local legislation could apply to the acquisition of cloud storage data.

Figure 255

Warning: Legislation could apply to the acquisition of cloud storage data

☐ Download Any Available Cloud Files

Currently supported files include the following:

- OneDrive
- Google Drive
- Dropbox

FILE CARVE (WINDOWS ONLY)

A file deleted from a computer usually hasn't been completely removed. To wipe all the data in a file, the disk would have to reset all bytes, taking a long time for larger files. The system marks the data as 'unallocated space' that can be used again to speed up the process.

However, there's so much space on modern storage devices that there's a good chance that any section of 'unallocated space' won't be needed for some time, leaving the deleted file on the device longer.

File carving works by scanning the raw bytes, reassembling them, and searching for the most recently deleted files.

Figure 256



NOTE! This job is only available on Detego Field for Windows devices.

Figure 257

File Carve

Target Drives

	Location	Model	Size	
☐	\\.\PHYSICALDRIVE0	NVMe WD PC SN735 SDBPTHH-1T00-1002	953.9GB	
☒	\\.\C:	OS	930.5GB	

Timeout

No Timeout

☒ Hash Matching ...

☐ Ignore Safe Hash Files (e.g. NSRL)

☒ Keyword Matching ...

TARGET DRIVES:

These are the available drives for File Carving.

- Select the drives you wish to perform File Carving on.

TIMEOUT:

This is the length of time before the File Carving job will stop if no data has been recovered.

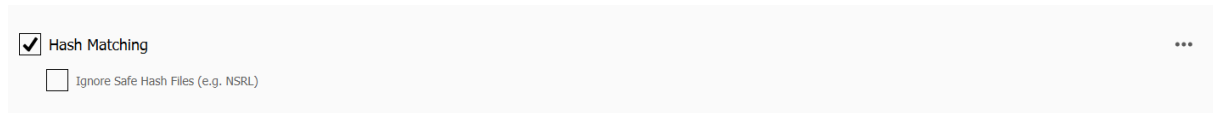
- Move the slider to specify how long you wish to have the timeout.

HASH MATCHING:

Hash Matching allows you to hash match the data you are extracting using your hashlists created from Detego Analyse.

- Select the checkbox next to Hash Matching in order to enable hash matching. This will open up the following section:

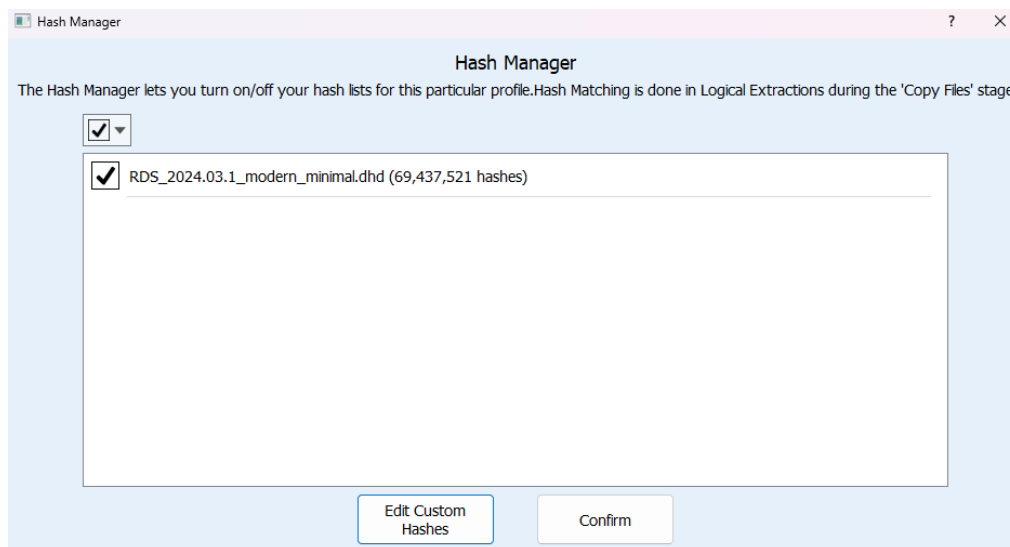
Figure 258



From here you can the following options:

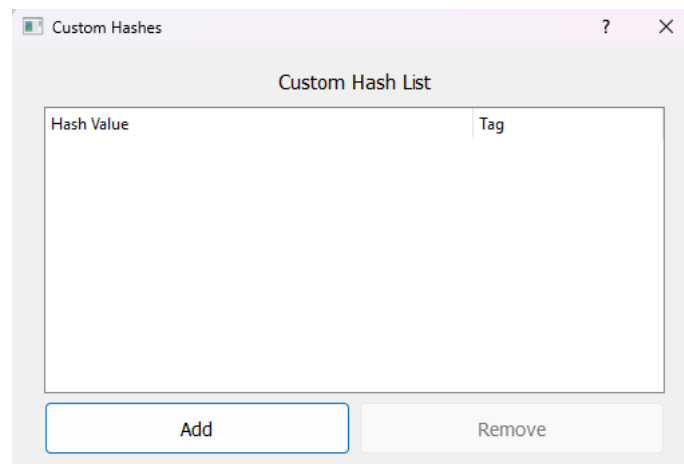
- **Ignore Safe Hash Files (e.g. NSRL)**
 - This will ignore any “safe” hashlists you have added e.g. NSRL. This means the extraction will not extract known safe hash files.
- If you wish to mange your hashlists or custom hashes, select the three dots menu “...” on the right of Hash Matching option to open the Hash Manager window:

Figure 259



- Simply select any hashlist you wish to run hash matching against.
- If you wish to edit your custom hashes, select the “Edit Custom Hashes” button. This will open the below window where you can add your custom hash:

Figure 260



KEYWORD MATCHING:

- If you wish to run Keyword Matching on the File Carve job, select the Keyword Matching checkbox and select which Keyword Lists you wish to match against.

Figure 261

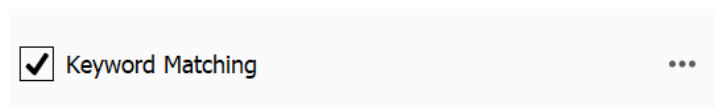
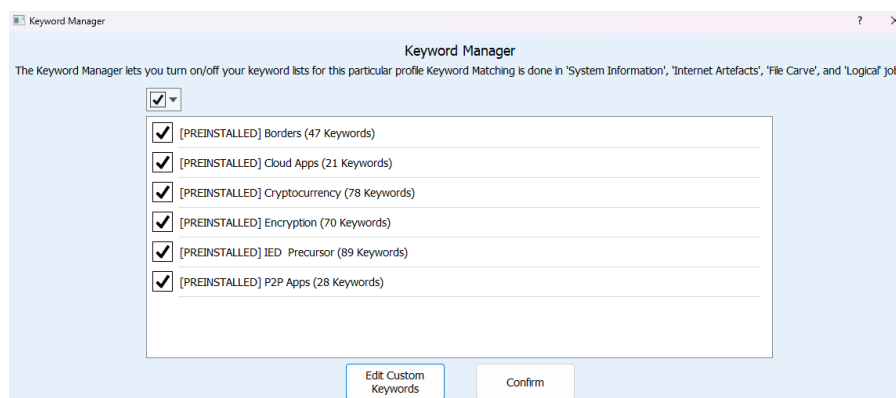
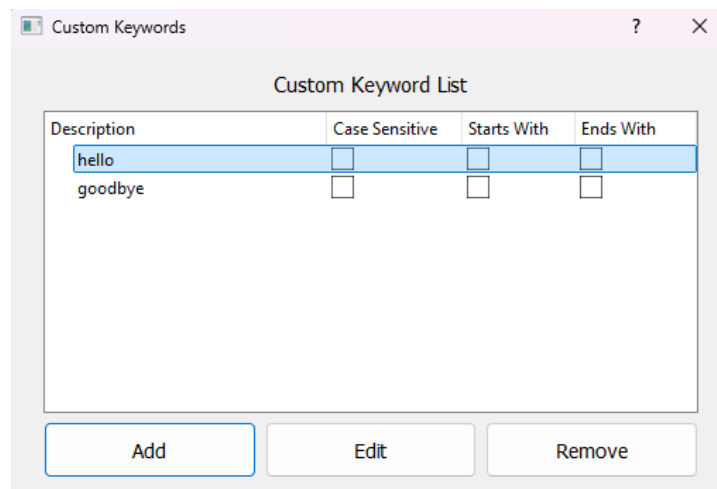


Figure 262



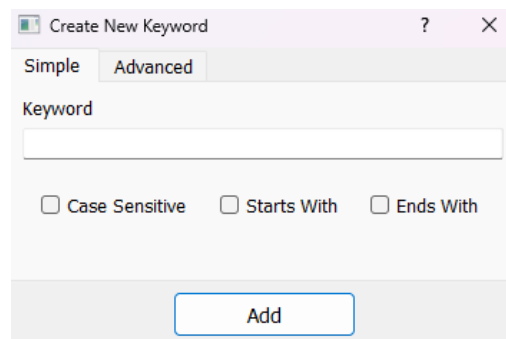
- If you would like to add, remove, or edit your custom Keywords, select the "Edit Custom Keywords".
- Once you have selected this, the below window will display:

Figure 263



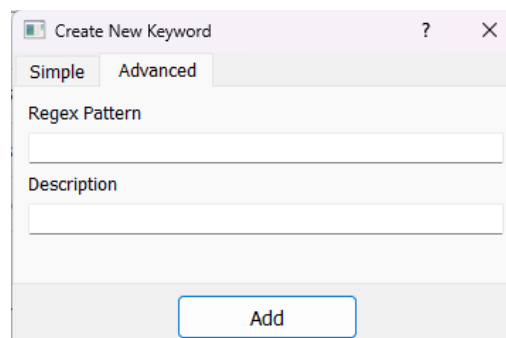
- Select Add to add a new Keyword. This will allow you to choose the following options:
 - **Simple Tab:**
 - **Keyword** - Type out your keyword.
 - **Case Sensitive** - Check this if you wish they keyword to be case sensitive.
 - **Starts With** - Allows Keyword Matching with words that have this keyword at the start.
 - **Ends With** - Allows Keyword Matching with words that have this keyword at the end.
 - **Advanced Tab:**
 - **Regex Pattern** - Input your Regex pattern.
 - **Description** - Describe the Regex pattern.

Figure 264



The dialog box titled "Create New Keyword" has a "Simple" tab selected. It contains a text input field labeled "Keyword". Below the field are three checkboxes: "Case Sensitive", "Starts With", and "Ends With". At the bottom is an "Add" button.

Figure 265



The dialog box titled "Create New Keyword" has an "Advanced" tab selected. It contains two text input fields: "Regex Pattern" and "Description". At the bottom is an "Add" button.

- Once you are happy with your selection, select the “Confirm” button to save your selection for this job.

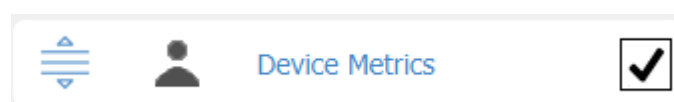
NOTE! Keyword Matching is completed on metadata because no carving process can recover filenames.

DEVICE METRICS

The Device Metrics job will automatically select the following jobs.

- System Information
- Password Finder
- Internet Artefacts

Figure 266

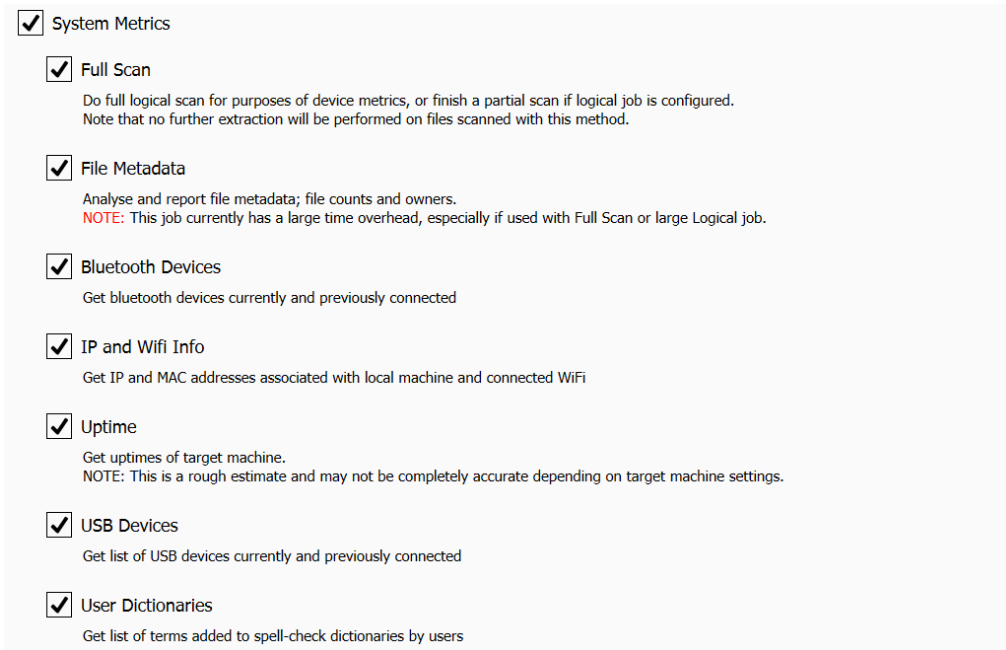


A horizontal bar with a list of jobs. The "Device Metrics" job is selected, indicated by a checkmark icon in a box on the right. To the left of the job name are icons for a list and a person.

SYSTEM METRICS:

The following options are available for the System Metrics section of the Device Metrics job:

Figure 267



The screenshot shows a configuration window for 'System Metrics'. It contains a list of options, each with a checked checkbox and a description. The options are: 'System Metrics', 'Full Scan', 'File Metadata', 'Bluetooth Devices', 'IP and Wifi Info', 'Uptime', 'USB Devices', and 'User Dictionaries'. Each option has a brief description and some have additional notes.

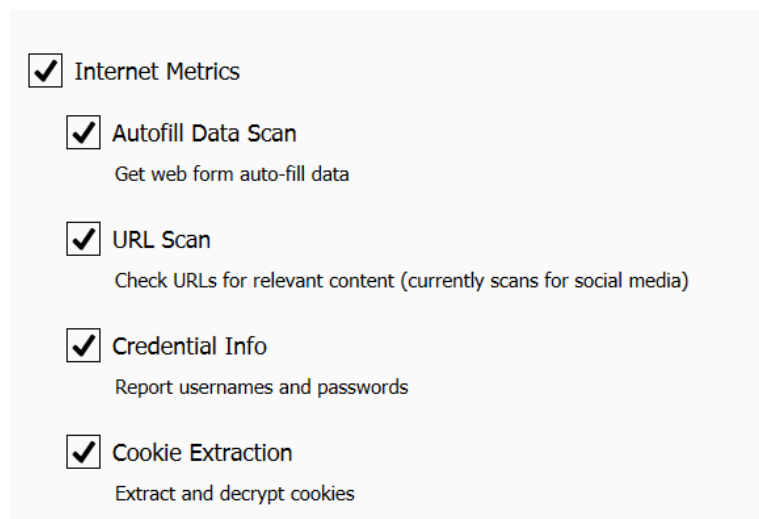
- ☒ **System Metrics**
- ☒ **Full Scan**
Do full logical scan for purposes of device metrics, or finish a partial scan if logical job is configured.
Note that no further extraction will be performed on files scanned with this method.
- ☒ **File Metadata**
Analyse and report file metadata; file counts and owners.
NOTE: This job currently has a large time overhead, especially if used with Full Scan or large Logical job.
- ☒ **Bluetooth Devices**
Get bluetooth devices currently and previously connected
- ☒ **IP and Wifi Info**
Get IP and MAC addresses associated with local machine and connected WiFi
- ☒ **Uptime**
Get uptimes of target machine.
NOTE: This is a rough estimate and may not be completely accurate depending on target machine settings.
- ☒ **USB Devices**
Get list of USB devices currently and previously connected
- ☒ **User Dictionaries**
Get list of terms added to spell-check dictionaries by users

- **Full Scan** - Do a full logical scan for purposes of device metrics, or finish a partial scan if logical job is configured. **NOTE!** No further extraction will be performed on files scanned with this method.
- **File Metadata** - Analyse and report file metadata, file counts and owners. **NOTE!** This job has a large time overhead, especially if used with Full Scan or large Logical job.
- **Bluetooth Devices** - Get bluetooth devices currently and previously connected.
- **IP and WiFi Info** - Get IP and MAC addresses associated with local machine and connected WiFi.
- **Uptime** - Get uptimes of target machine. **NOTE!** This is a rough estimate and may not be completely accurate depending on target machine settings.
- **USB Devices** - Get list of USB devices currently and previously connected.
- **User Dictionaries** - Get list of terms added to spell-check dictionaries by users.

INTERNET METRICS:

The following options are available for the Internet Metrics section of the Device Metrics job:

Figure 268



☒ Internet Metrics

☒ Autofill Data Scan
Get web form auto-fill data

☒ URL Scan
Check URLs for relevant content (currently scans for social media)

☒ Credential Info
Report usernames and passwords

☒ Cookie Extraction
Extract and decrypt cookies

- **Autofill Data Scan** - Get web form auto-fill data.
- **URL Scan** - Check URLs for relevant content (currently scans for social media).
- **Credential Info** - Report usernames and passwords.
- **Cookie Extraction** - Extract and decrypt cookies.

Additional Registry keys will be extracted. Once complete, all results will appear in a 'Personally Identifiable Information Report' report.

PHYSICAL IMAGE / BALLISTIC EXTRACTION

Detego Field is designed so that the operator can rapidly gather information in as few steps as possible. Typically, the best way to approach this is by targeting the most critical files and parsing them to gather valuable data. Sometimes, an investigation will require a more thorough search; this is where a "Physical Image" comes in.

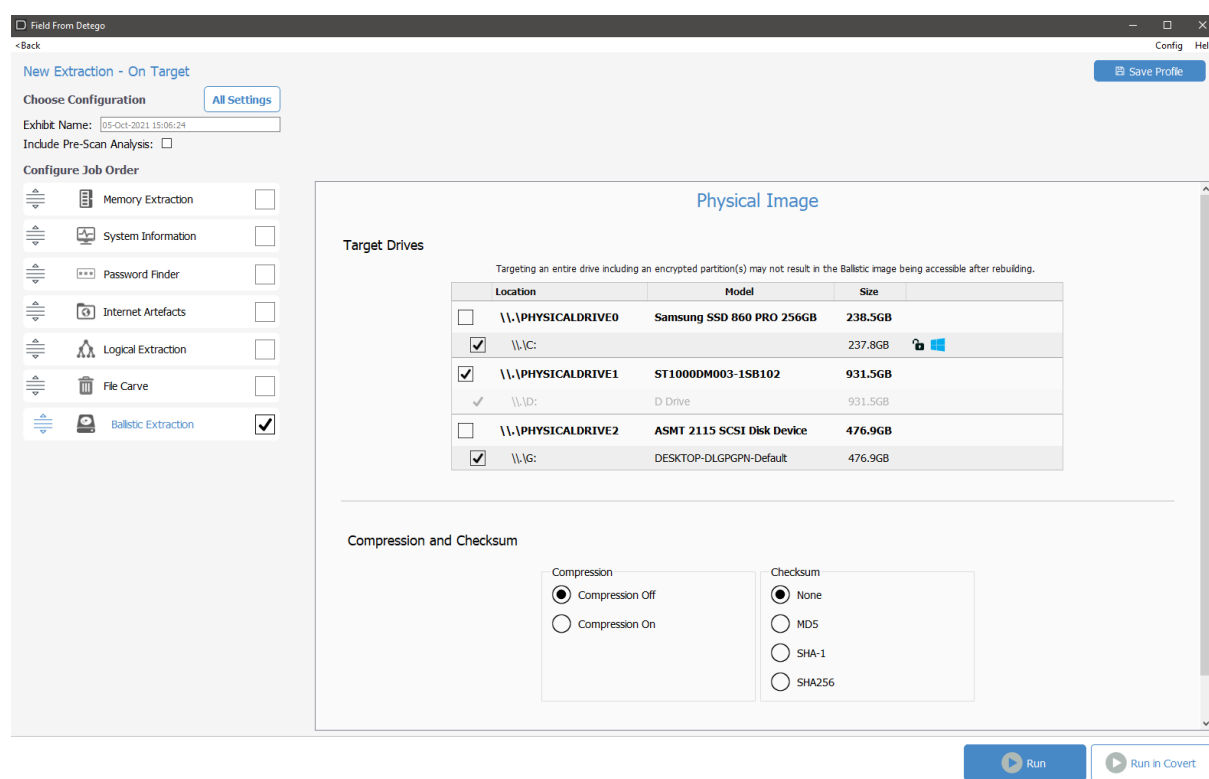
There are two methods of extracting a physical image. The first is a basic Physical Image which can be accessed in Detego Field. The second is a Ballistic Extraction which is Detego's superfast imaging tool. (If you do not have access to Ballistic Imager, contact marketing@detegoglobal.com).

PHYSICAL IMAGE

This job targets a storage drive and makes an exact bit-for-bit copy. This physical image contains the entire file system, with all files, metadata, and recoverable deleted files. Once off the target machine, you can perform as many forensic tasks as possible.

You can select the specific physical drives you want to image by choosing them from the list of drives connected to your target machine. There are two options available when performing the physical image job.

Figure 269



A Detego logo will appear next to drives that either have Detego Analyse installed or are recognised as a Field Device. The right-click option is available to hide unavailable drives.

Compression - this will compress the file if collection space is an issue. For Maximum Speed, leave compression turned off. It is off by default.

- **Checksum** - A hash value will be calculated for the entire disk image for validation purposes. For Maximum Speed, leave the checksum turned off. It is set to None by default.

EXTRACTING INDIVIDUAL ENCRYPTED PARTITIONS

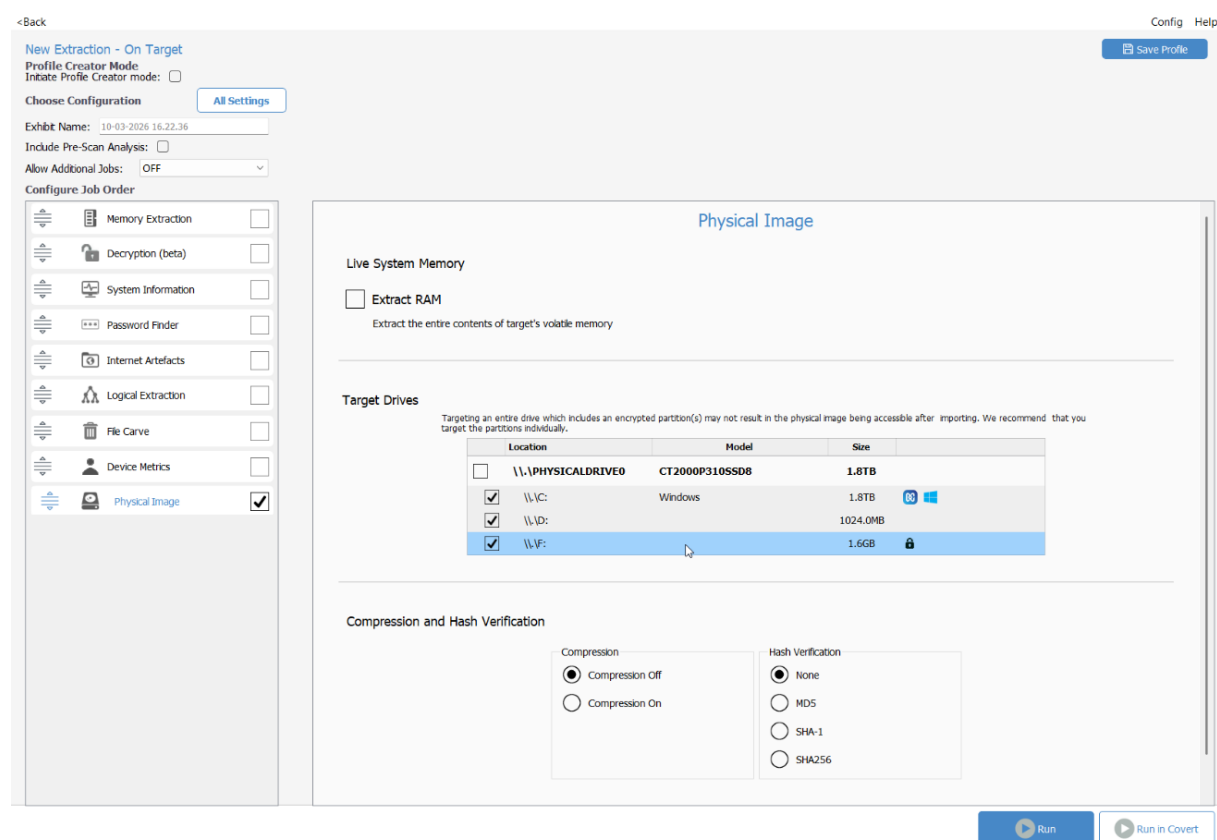
Due to the complexities of extracting encrypted data from individual partitions, this section assists with imaging the drives.

Note: You need the BitLocker password or recovery key to extract data using Detego Analyse.

Please follow the below steps:

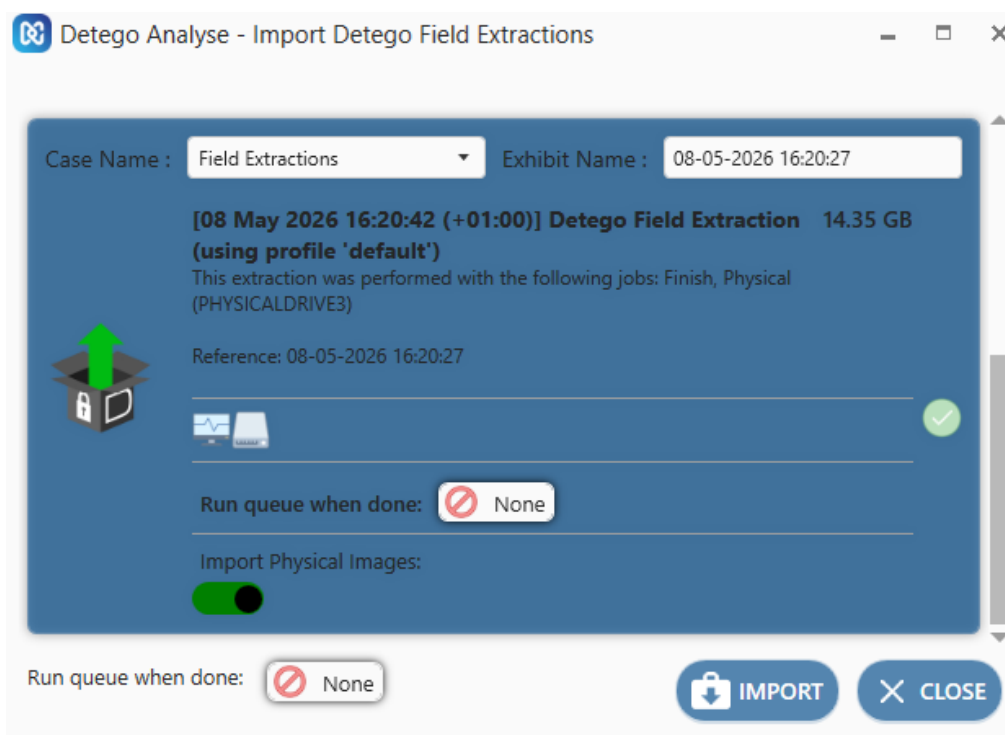
- Within the Create New Profile option in Detego Field, select Ballistic/Physical Image job.
- Within Ballistic/Physical Image, select the Target Drive you want to image.

Figure 270



- Run the extraction.
- When you import into Detego Analyse, in the Import window, select the Import and then Import Physical Images.
- Select IMPORT.

Figure 271



Once you have imported, you can follow the steps in **Analyse and Manage** under **BitLocker Physical Image Decrypter**. This will allow you to decrypt the image using the password or recovery key, allowing you to extract from and analyse further.

LOAD PROFILE/RUN RECENT

This option allows the user to load custom profiles that they previously configured and saved on their Field device. Refer to the section for instructions on configuring and saving your custom profiles. If you have custom profiles that you created and saved on your Field device, they will appear on the left under the 'Most Recent Profile'. The window on the right shows the jobs contained in your selected profile.

Figure 272

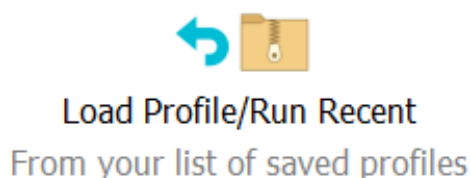
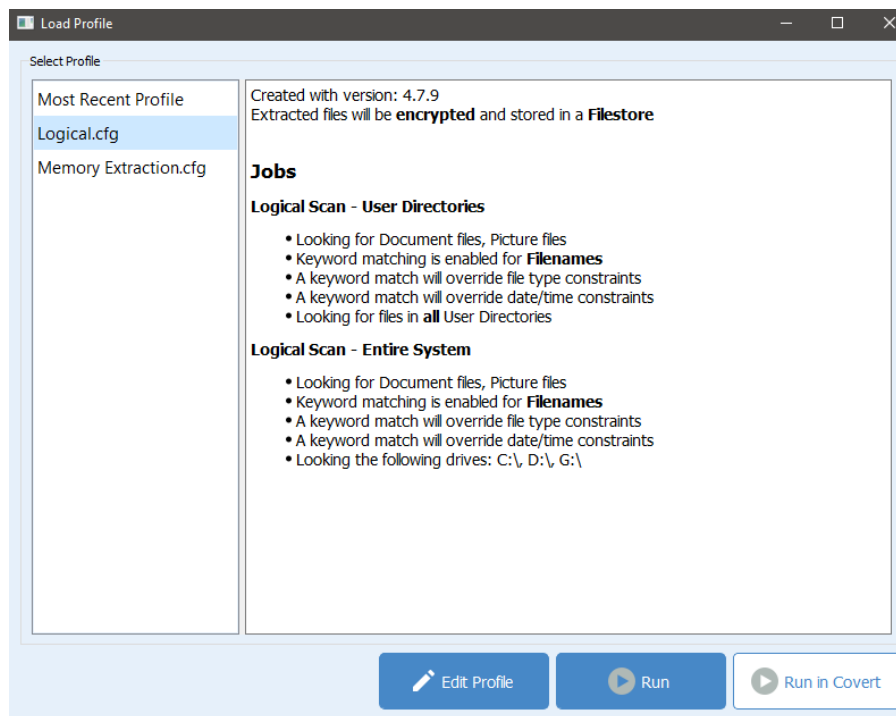


Figure 273



You can change your selected profile by clicking on the 'Edit Profile' button at the bottom of the window or immediately run the profile by clicking on 'Run Profile.'

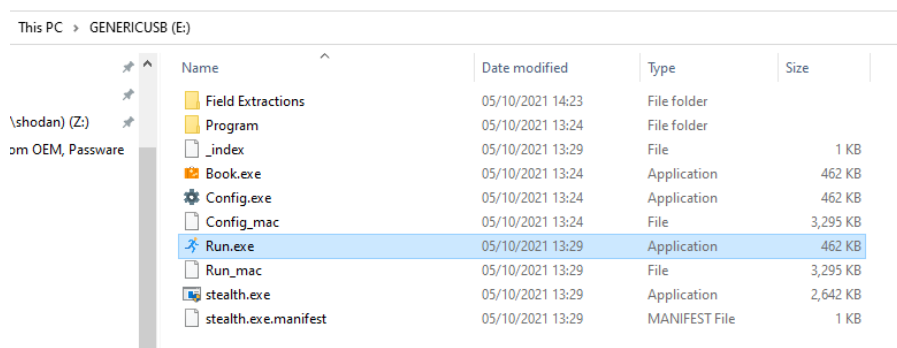
If Case Notes were entered on creation, they will appear here.

To run the most recently used profile, follow these steps:

- Select the 'Run Most Recent Profile' tool tile from the Detego Config window.
- The 'Load Profile' pop-up will appear with a list of jobs run during the last Field extraction performed by that Field device.
- Clicking the 'Edit Profile' button will allow the user to customise the extraction job(s) and save it as a custom profile or run it immediately. Clicking the 'Run Profile' button begins the acquisition.

Note: If in a time-pressured environment, the operator can double-click the 'Run.exe' shortcut from the root of the Field device (Right-click and 'Run as Administrator'). This will also run the most recently used acquisition profile.

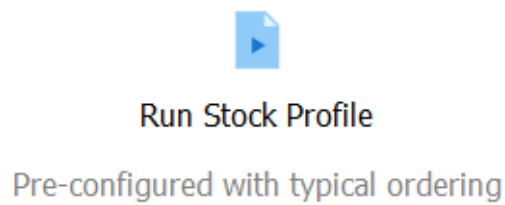
Figure 274



Name	Date modified	Type	Size
Field Extractions	05/10/2021 14:23	File folder	
Program	05/10/2021 13:24	File folder	
_index	05/10/2021 13:29	File	1 KB
Book.exe	05/10/2021 13:24	Application	462 KB
Config.exe	05/10/2021 13:24	Application	462 KB
Config_mac	05/10/2021 13:24	File	3,295 KB
Run.exe	05/10/2021 13:29	Application	462 KB
Run_mac	05/10/2021 13:29	File	3,295 KB
stealth.exe	05/10/2021 13:29	Application	2,642 KB
stealth.exe.manifest	05/10/2021 13:29	MANIFEST File	1 KB

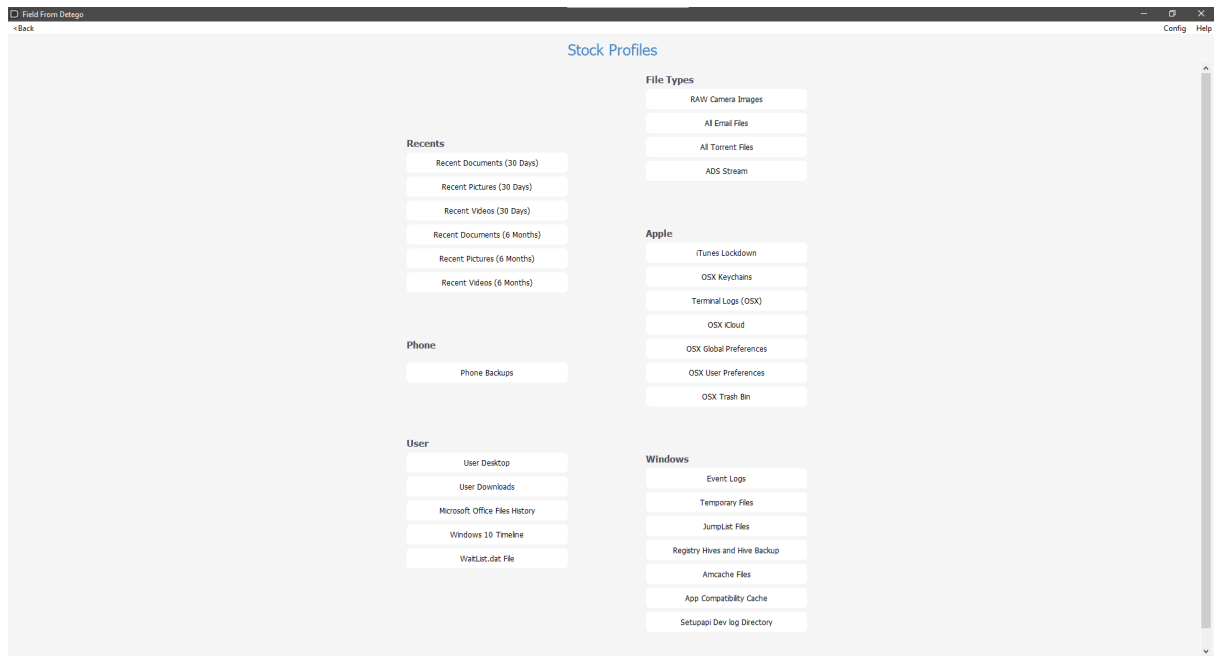
RUN STOCK PROFILE

Figure 275



Detego Field ships with several pre-built profiles that cover common extraction tasks. If necessary, these can be edited from the Field master device.

Figure 276



RECENT

- **Recent Documents (30 Days)** – Performs a logical extraction of only document files created or modified in the last 30 days.
- **Recent Pictures (30 Days)** – Performs a logical extraction of only picture files created or modified in the last 30 days.
- **Recent Videos (30 Days)** – Performs a logical extraction of only video files created or modified in the last 30 days.
- **Recent Documents (6 Months)** – Performs a logical extraction of only document files created or modified in the last six months.
- **Recent Pictures (6 Months)** – Performs a logical extraction of only picture files created or modified in the last six months.
- **Recent Videos (6 Months)** – Performs a logical extraction of only video files created or modified in the last six months.

PHONE

- **Phone Backups** – Performs a search for backup directories for known phone backup file formats.

USER

- **User Desktop** – Targets each Windows user's desktop, extracting every file.
- **User Downloads** – Targets each Windows user's downloads folder, extracting every file.
- **Microsoft Office Files History** – Targets Microsoft Office File History, extracting every file found there.
- **Windows 10 Timeline** – Targets the Windows Timeline for each Windows 10 user and extracts all data.
- **WaitList.dat File** – Targets and extracts from the WaitList.dat File.

FILE TYPES

- **RAW Camera Images** – Performs a logical extraction for all RAW camera files.
- **All Email Files** – Performs a logical extraction of all known email files.
- **All Torrent Files** – Performs a logical extraction on only P2P Torrent links.
- **ADS Stream** – Extracts all data from the ADS stream.

APPLE

- **iTunes Lockdown** – Targets the iTunes Lockdown Directory and extracts all files.
- **OSX Keychains** – Targets the OSX Keychain Directory and extracts all files.
- **Terminal Logs (OSX)** – Performs a 'System Profile' scan, searching each user for 'bash history' files.
- **OSX iCloud** – Targets the OSX iCloud directory and extracts all files.
- **OSX Global Preferences** – Targets the OSX Global Preferences and extracts all files.

- **OSX User Preferences** – Targets the OSX User Preferences and extracts all files.
- **OSX Trash Bin** – Targets the OSX Trash Bin and extracts all files.

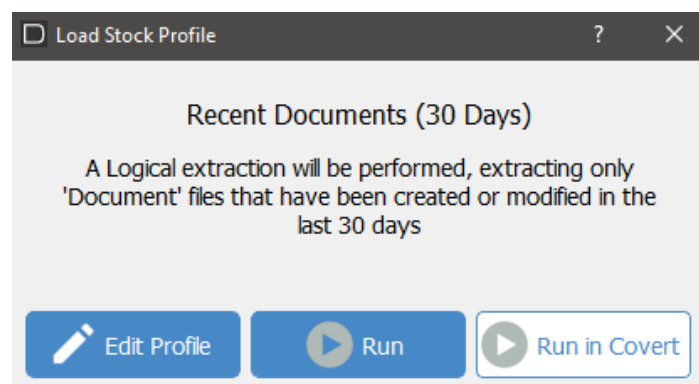
WINDOWS

- **Event Logs** – Targets the event log directory and extracts all files. It also extracts the registry hives and hive backups.
- **Temporary Files** – Targets the temporary files for each Windows user and extracts all files.
- **JumpList Files** – Targets and extracts all JumpList files.
- **Registry Hives and Hive Backup** – Targets the Registry Hive and Hive Backup and extracts all data.
- **Amcache Files** – Targets and extracts all Amcache files.
- **App Compatibility Cache** – Targets and extracts all the App Compatibility Cache data.
- **Setupapi Dev log Directory** – Targets and extracts all data from the Setupapi Dev log Directory.
- **Windows Recycle Bin** – Targets and extracts all data from the Windows Recycle Bin.

To run a stock profile, follow these steps:

- Select a profile to extract by clicking on the stock profile button.
- This will open a pop-up containing a short description of the selected pre-configured profile.

Figure 277



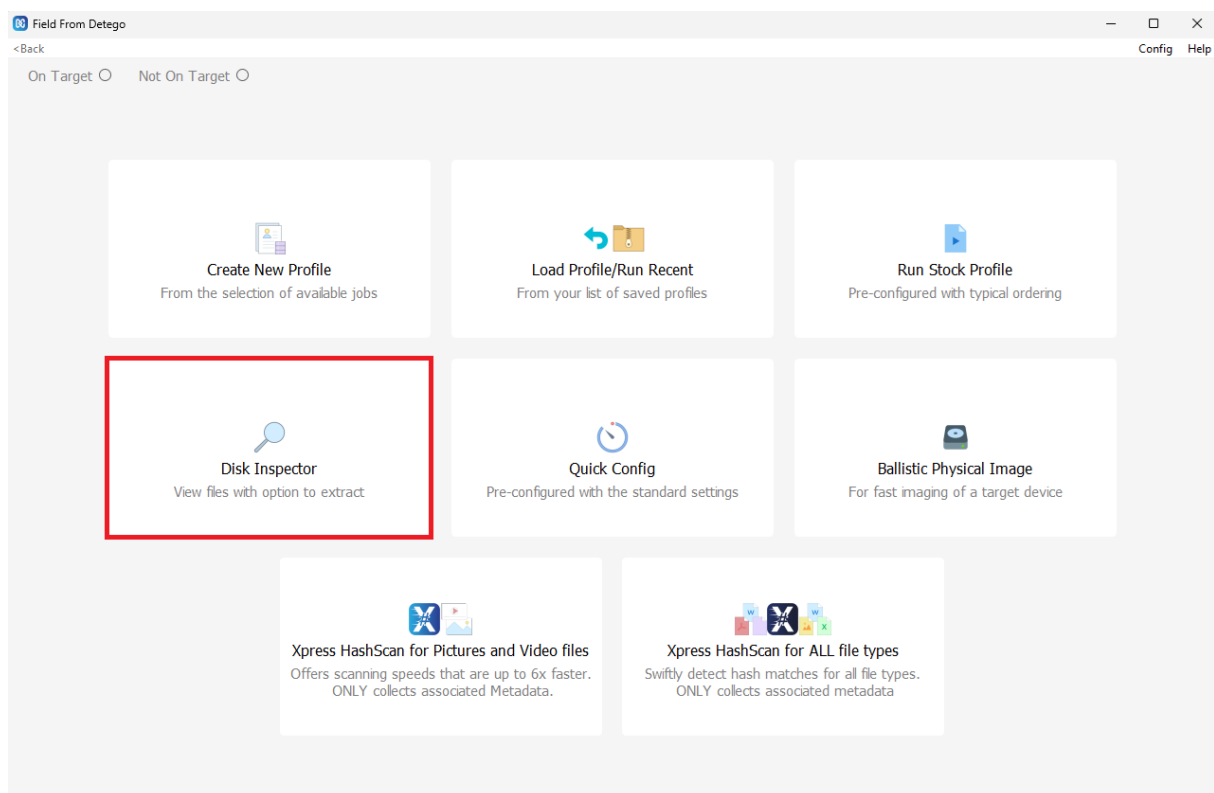
- Clicking the 'Edit Profile' button will allow the user to customise the extraction job(s) and save it as a custom profile or run it immediately. Clicking the 'Run Profile' button begins the acquisition.

DISK INSPECTOR IN DETEGO FIELD

Disk Inspector is a feature that allows viewing the target device's file system and selecting folders to extract.

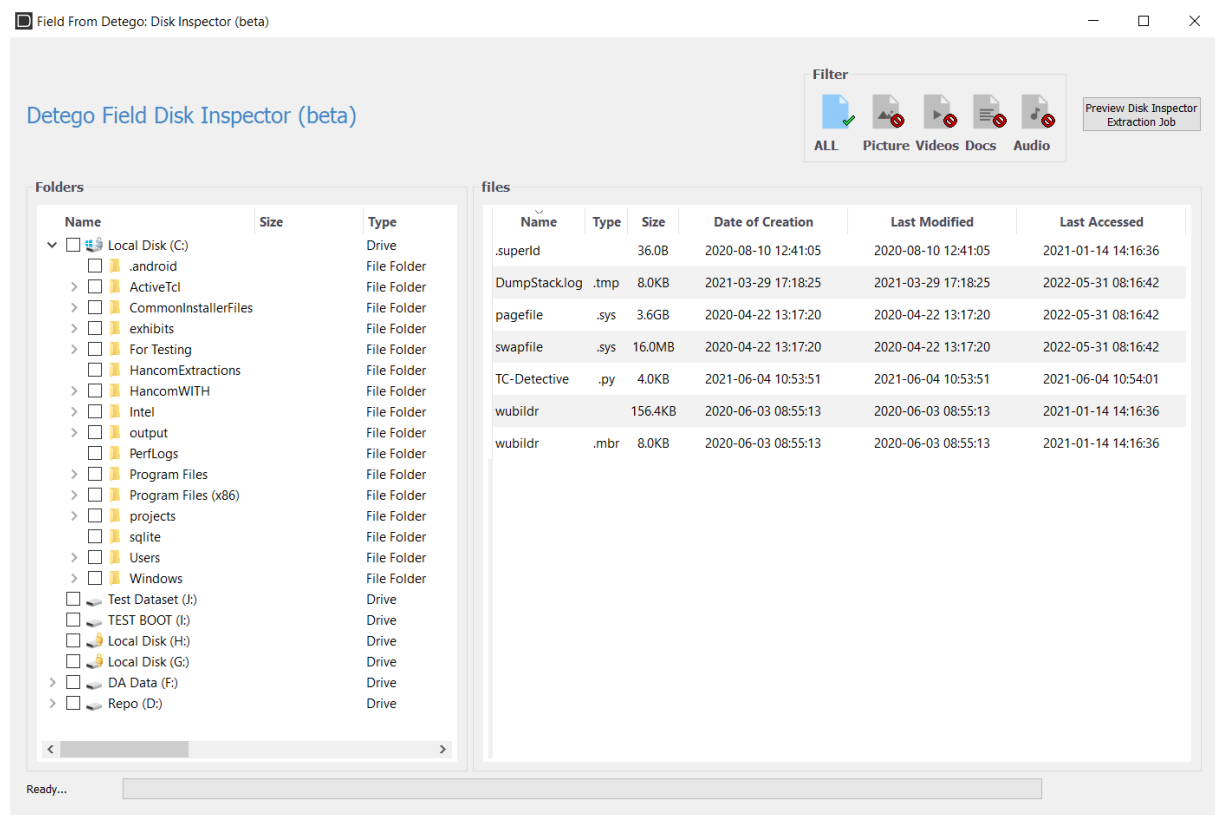
- From the Home Screen of the Field device, select 'Disk Inspector.'

Figure 278



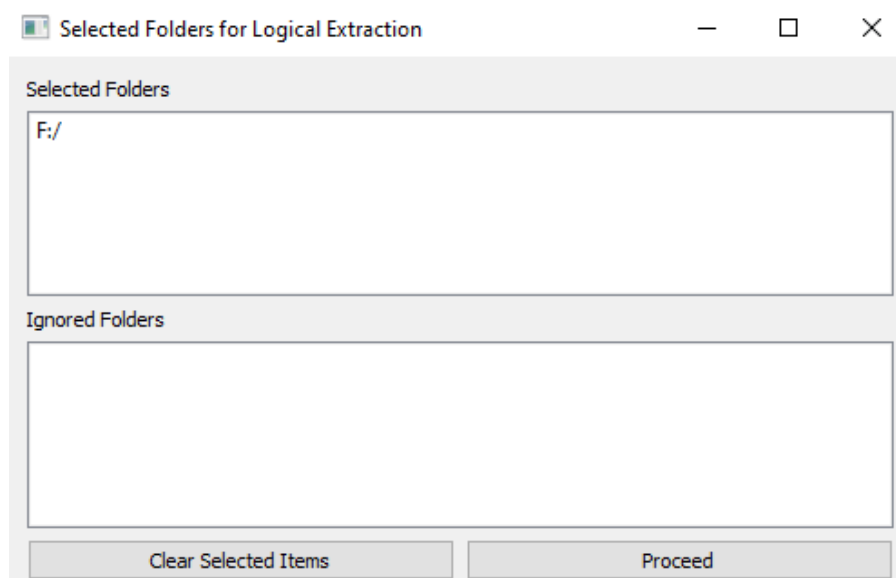
- This will bring up the Disk Inspector Window.

Figure 279



- Select any folder(s) you wish to extract from this window, then select the 'Preview Disk Inspector Extraction Job' button in the top right corner.

Figure 280



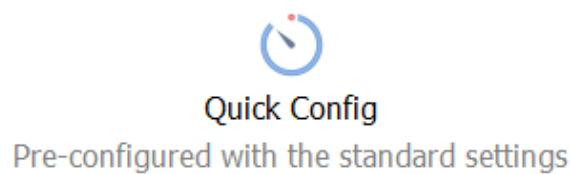
- You can see all selected files and folders and ignored ones from here. Press Proceed when you are happy with your selection.

- You will automatically be taken to the Logical Extraction screen, where your selected files and folders will be ready to extract.

QUICK CONFIG

The Quick Start profile is the fastest way to get actionable intelligence in as few steps as possible. Clicking on the quick Config allows the user to run the Field jobs of Memory Extraction, Password Finder, Logical Extraction, System Information, Internet Artefacts, File Carve and Physical/Ballistic Image, all using default settings if you are in a time-sensitive situation where you need to acquire information rapidly then this is the tool for you.

Figure 281



To run a profile using 'Quick Start', follow these steps:

- Click on the Detego Config window on the 'Quick Start' tool tile.
- The 'Quick Config' window will appear as shown below.

Figure 282

Quick Config

Exhibit Name: 12-10-2022 11:09:43

The quick config preset options are based on typical settings - please use the full configuration to optimise for specific extractions or speed

Memory Extraction	☐	System Information	☐
Password Finder	☐	Internet Artefacts	☐
User Directory Scan Logical Extraction	☐	Entire Disk Scan Logical Extraction	☐
File Carve	☐	Ballistic Image	☐

Run Run in Covert

Enter an Exhibit name; this will carry across to Detego Analyse once you import the extraction.

- Select the required job(s) to be run. You can change the options for some of the jobs before selecting the next job.

Note, if you do not have a Detego Ballistic Imager licence, you will see the 'Physical Image' option instead of 'Ballistic Image.'

BALLISTIC PHYSICAL IMAGE / PHYSICAL EXTRACTION

Detego Field is designed so that the operator can rapidly gather information in as few steps as possible. Typically, the best way to approach this is by targeting the most critical files and parsing them to gather valuable data. Sometimes, an investigation will require a more thorough search; this is where a 'Physical Extraction' comes in.

If you do not have Detego Ballistic Imager licensed, you will see 'Physical Extraction' instead of 'Ballistic Physical Image'. This is the same process; however, the Ballistic Imaging will allow multiple collectors for maximised imaging speeds.

This job targets a storage drive and makes an exact bit-for-bit copy. This physical image contains the entire file system, with all files, metadata, and recoverable deleted files. Once off the target machine, you can perform as many forensic tasks as possible.

You can select the specific physical drives you want to image by choosing them from the list of drives connected to your target machine.

There are two options available when performing the physical image job.

Figure 283

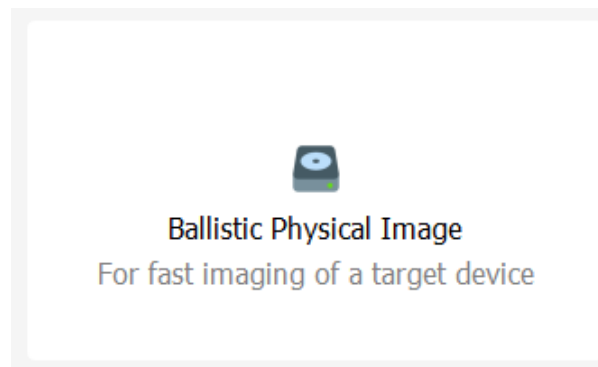
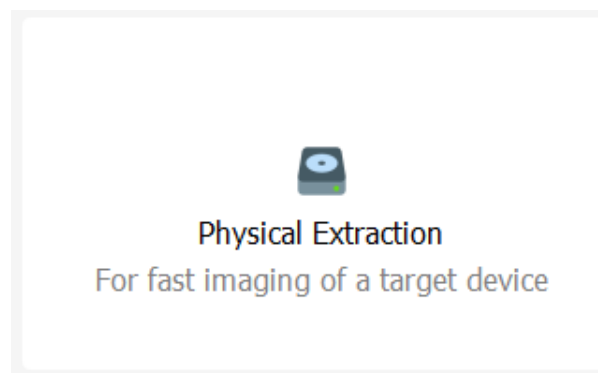
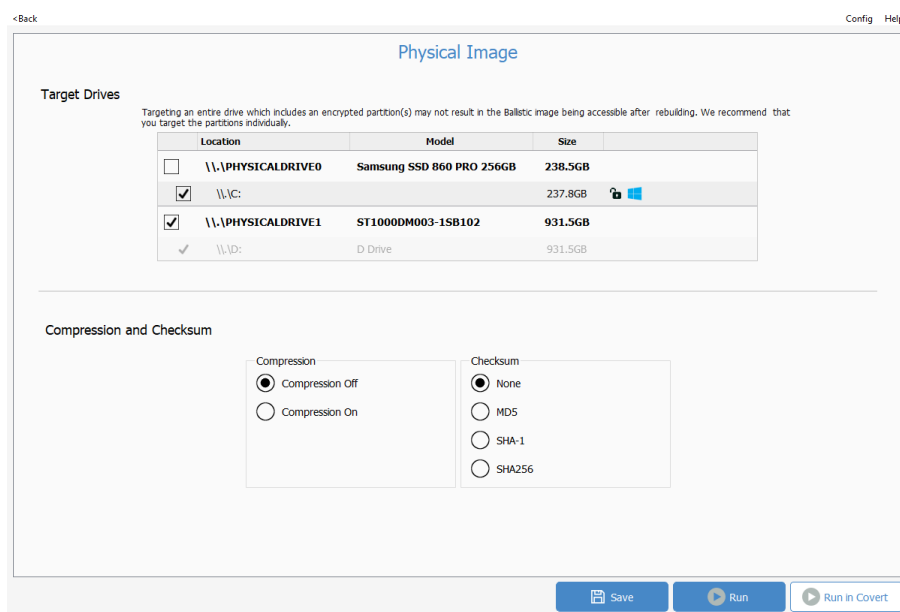


Figure 284



- Select the tile that reads 'Ballistic Physical Image' or 'Physical Extraction' from the Detego Field Home screen.
- From the next screen, you will see the available Target Drives for your physical Image job.

Figure 285



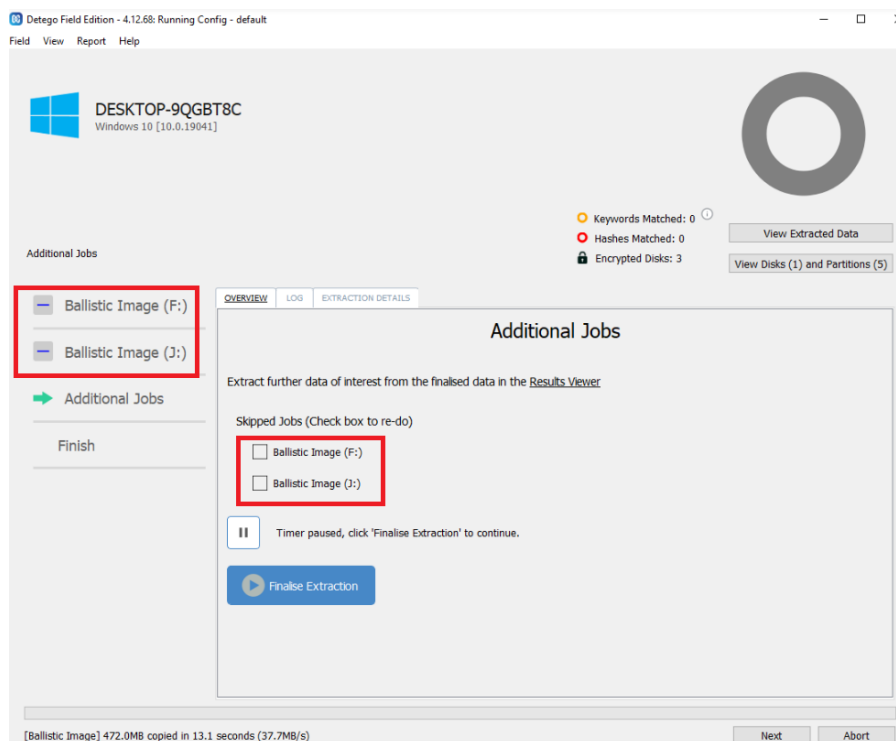
A Detego logo will appear next to drives that either have Detego Analyse installed or are recognised as a Field Device. The right-click option is available to hide unavailable drives.

- **Compression** - this will compress the file if collection space is an issue. For Maximum Speed, leave compression turned off. It is off by default.
- **Checksum** - will calculate a hash value for the entire disk image for validation purposes. For Maximum Speed, leave the checksum turned off. It is set to None by default.

When extracting, you can now pause or abort and resume from the last position in Ballistic.

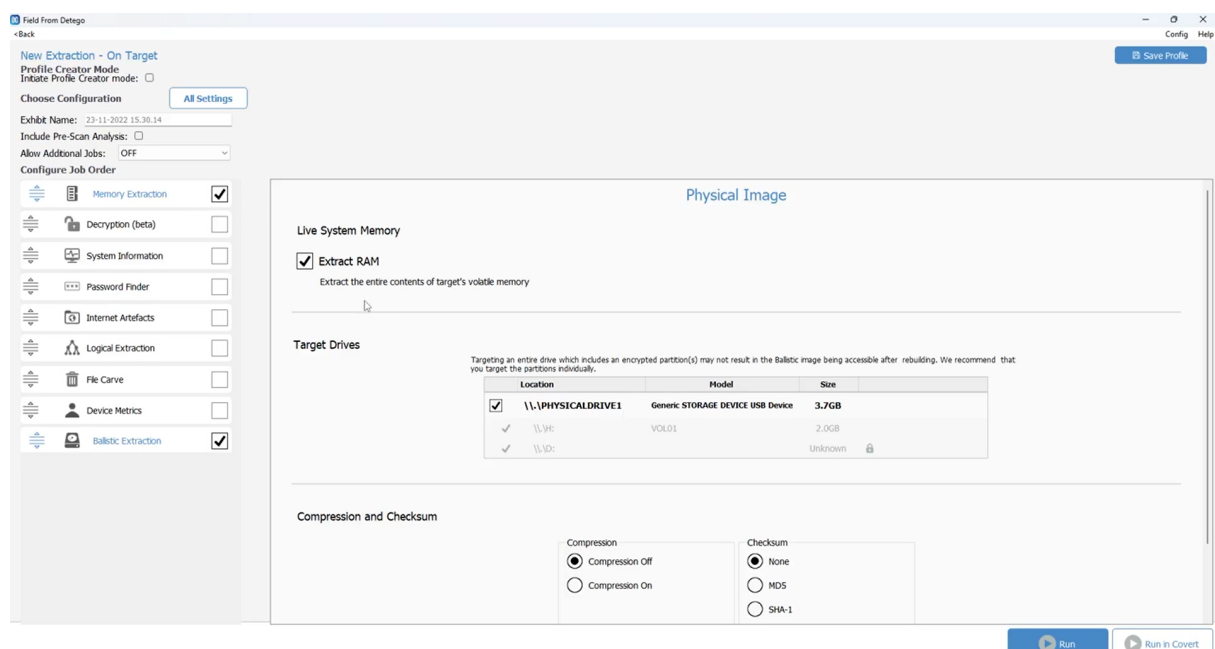
This allows for the Ballistic job to be continued from its previous position.

Figure 286



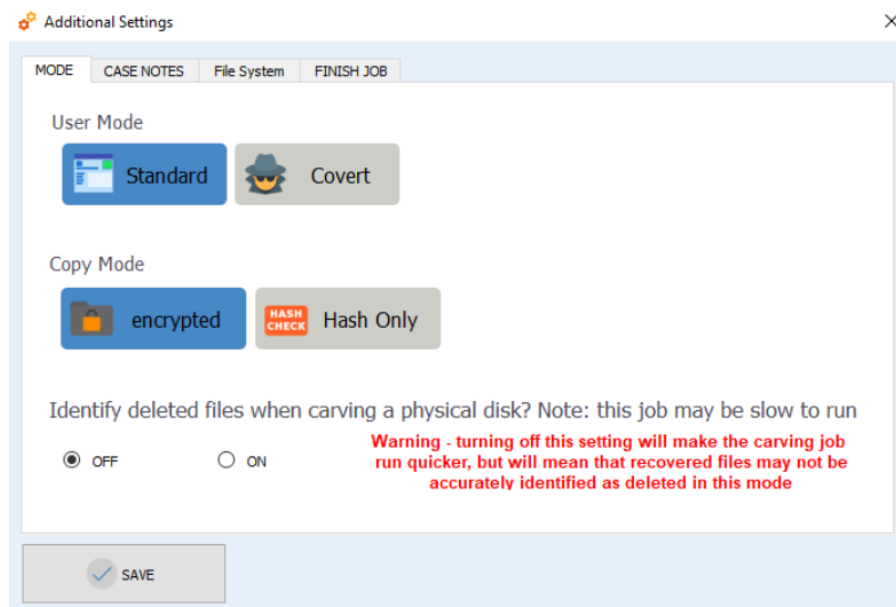
Selecting the RAM extraction from within the Ballistic Overview page is an option. Detego Analyse will check when clicking on RAM in Detego Analyse; if the RAM processor is not scheduled, suggests doing so.

Figure 287



Field Identifies which files are allocated (live) and unallocated (deleted) and marks them as such using the 'Recovery Source' property.

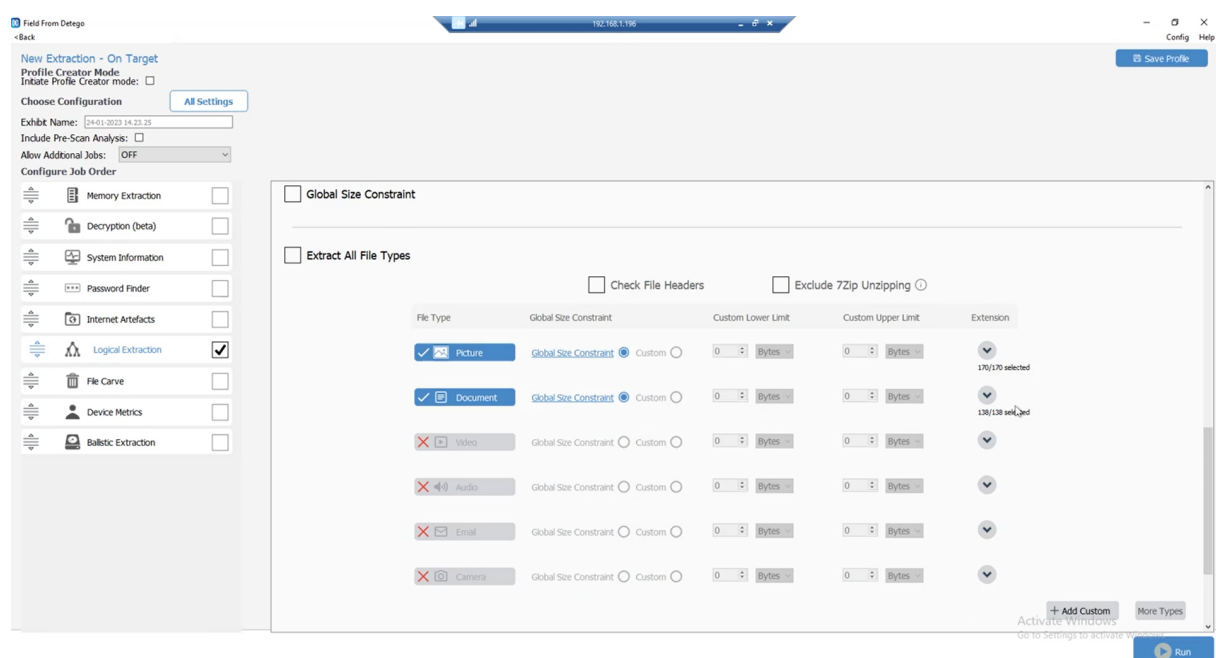
Figure 288



LOGICAL EXTRACTION

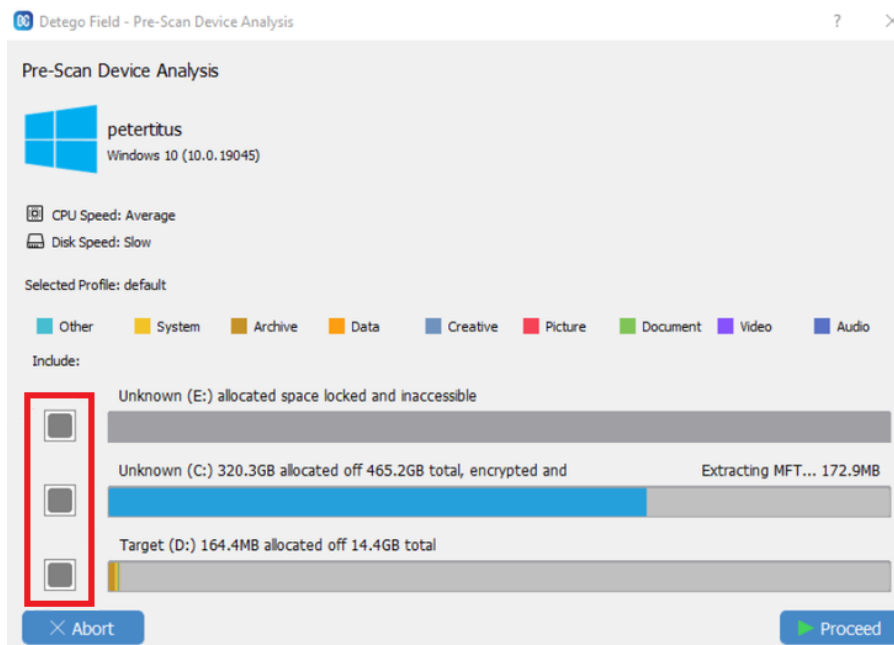
The Detego Field Logical File Extension selection shows the count of extensions, e.g. "170/170."

Figure 289



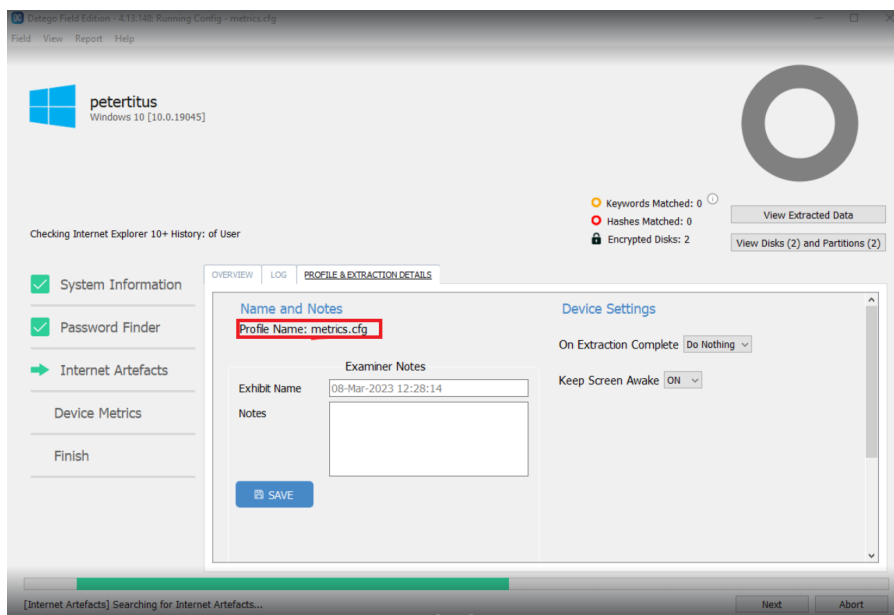
From the Pre-Scan Device Analysis, you can tick Disk within the Pre-Scan For Logical jobs.

Figure 290



When running Detego Field, it shows on the screen and logs the profile name as below:

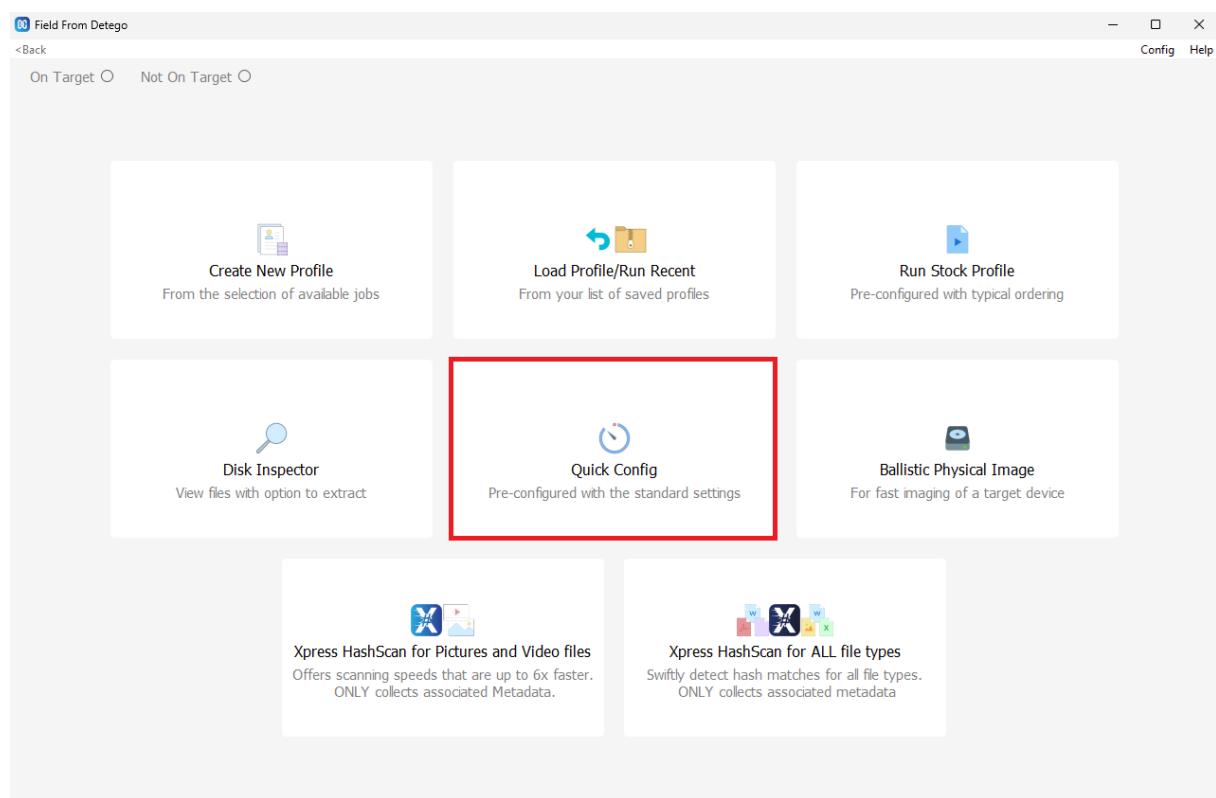
Figure 291



QUICK CONFIG

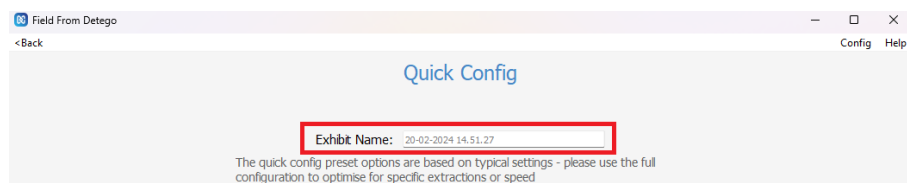
The 'Quick Config' option is used to put together jobs quickly if they have not been put together in a profile already. This is good for users who want to quickly configure a basic set up for Field.

Figure 292



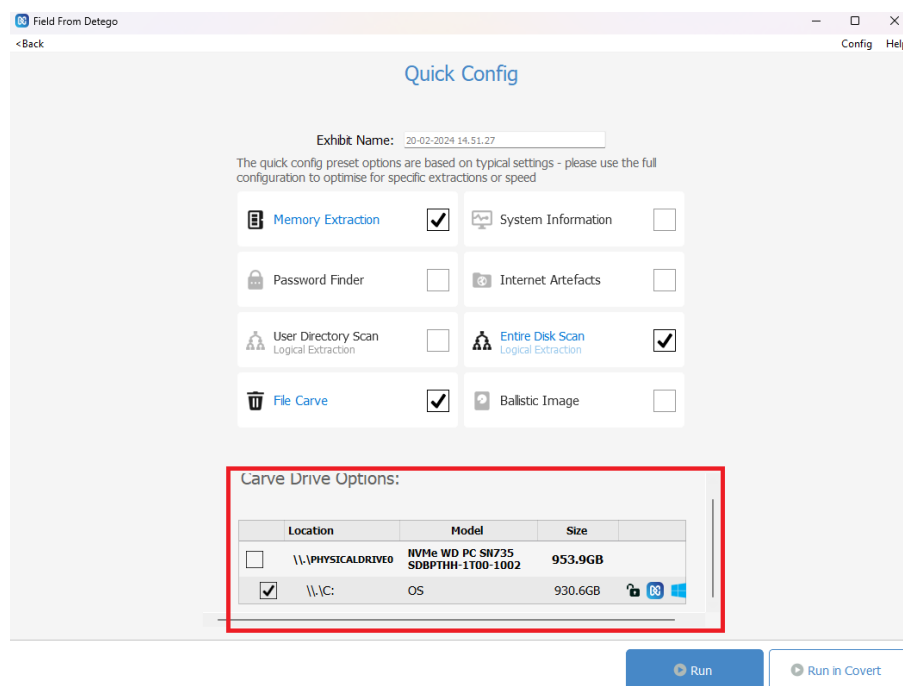
- You can give the extraction a name.

Figure 293



- Each Job that is selected may be able to be configured to the needs of the extraction. These options appear under the job selection and change when adding new jobs.

Figure 294



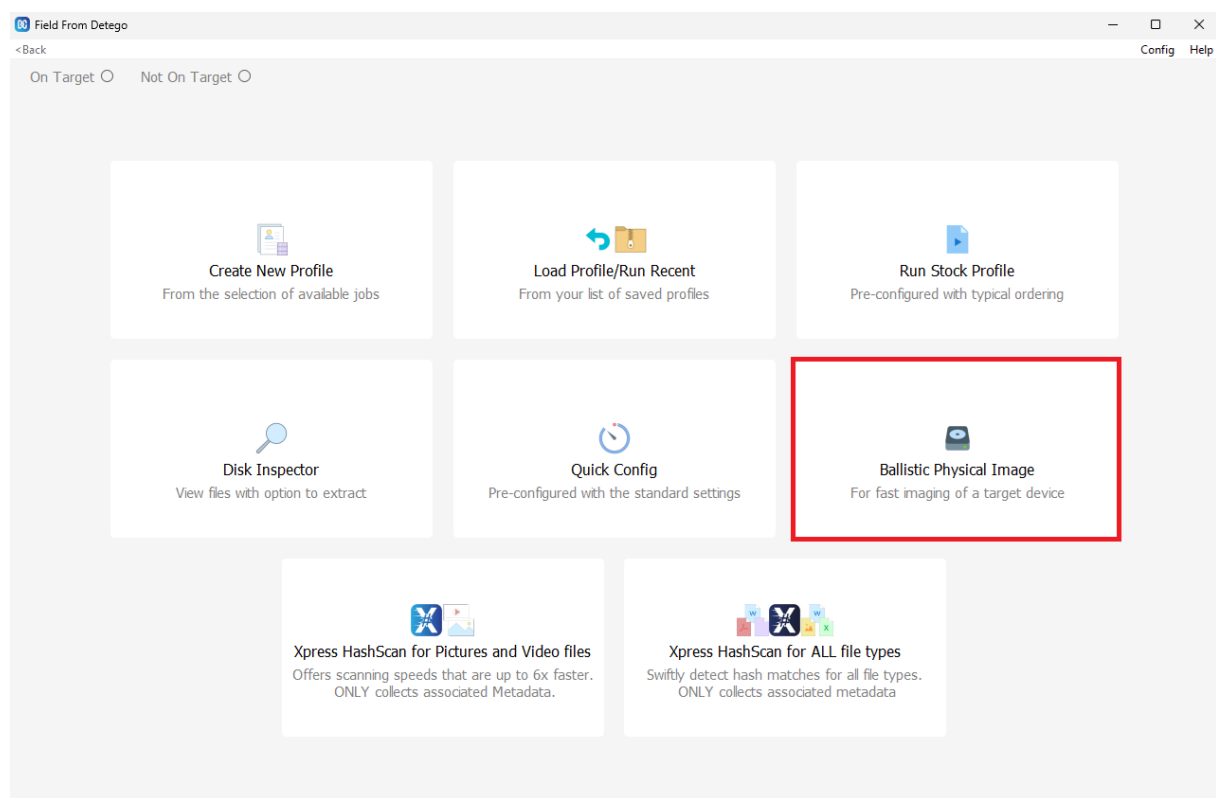
- Once the jobs have been selected and configured they can be 'Run'.

Note: This job selection does not get saved.

BALLISTIC PHYSICAL IMAGE

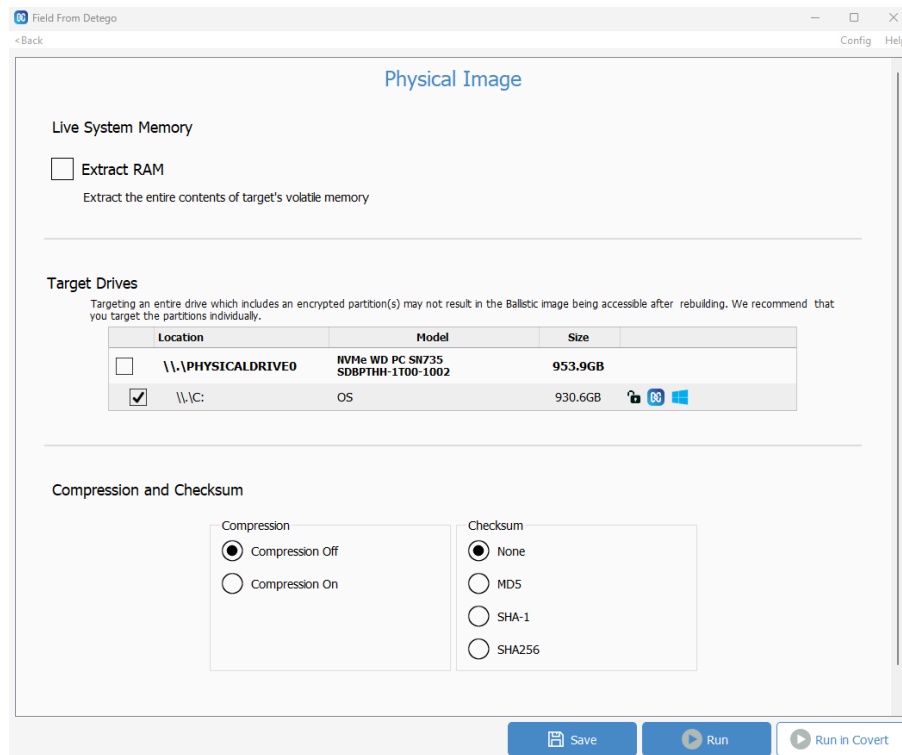
This job allows you to run a Ballistic Physical Image.

Figure 295



- You are able to configure the Ballistic Image using the settings provided.
 - Live System Memory: Extract the entire contents of the target machines volatile memory
 - Target Drives: Select which drive or drives you wish to extract
 - Compression and Checksum: Choose to compress the extraction or not. Then choose a file type you need the checksum in, if any.

Figure 296



- You are able to save this configuration as it's own profile for use again later.

XPRESS HASHSCAN MODES

In the **Xpress HashScan for Pictures and Video files mode**, the user can scan Media files much faster by only checking for hash matches for those media files (e.g., pictures and videos) without checking file headers, cloud files, or inside archive/links files. No keyword matching or file type selection is permitted for this Xpress HashScan mode. The user can also tell the HashScan to search through files that do not have a file extension if required. This is defaulted to off.

The **Xpress HashScan for ALL file Types mode** allows the user to scan all file types for hash matches without checking file headers, cloud files, or inside archive/link files.

Figure 297

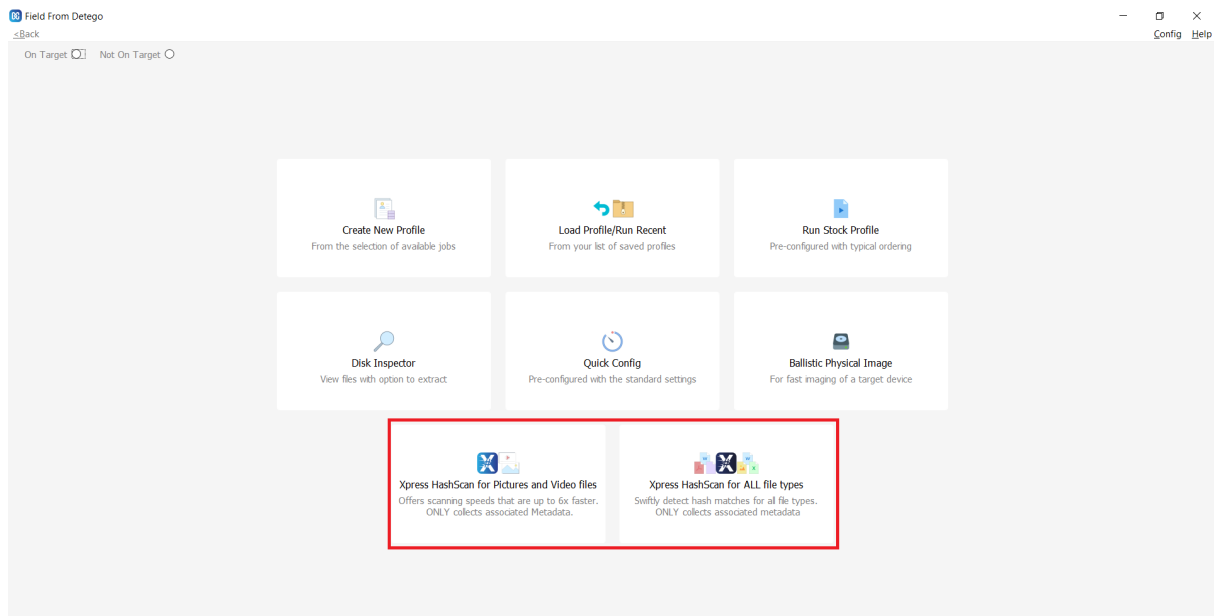
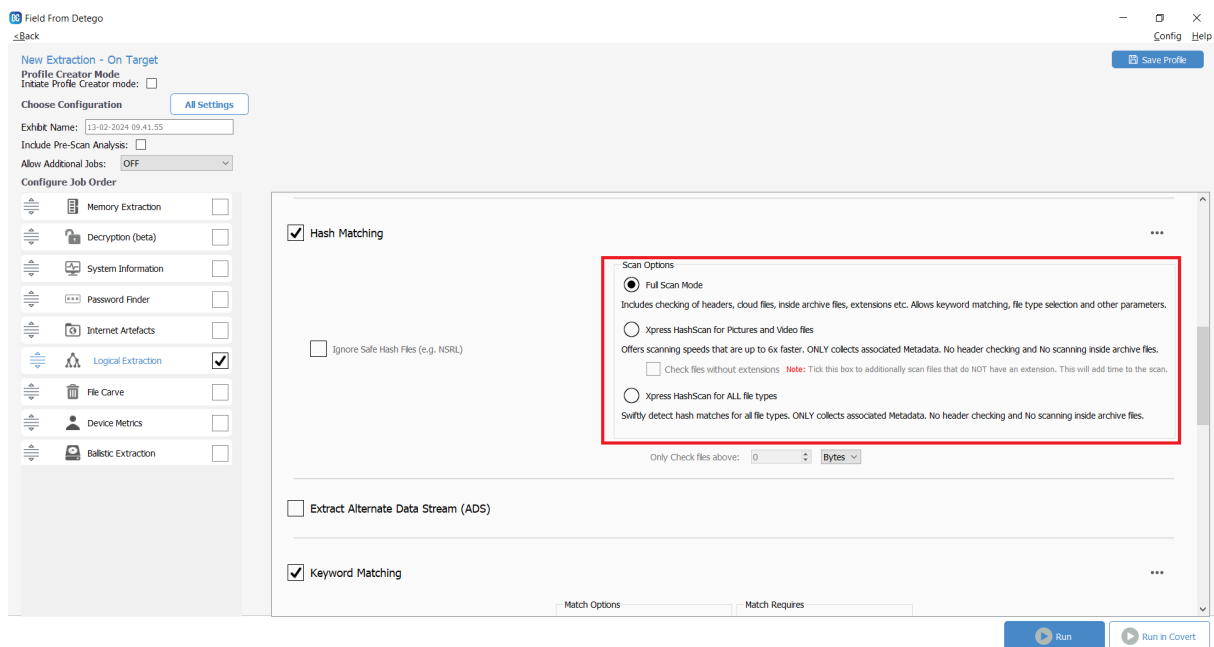


Figure 298



5.10. DETEGO HASHLIST CONVERTER

This section applies to: 'Detego Field for Mac' and 'Detego Field Legacy for Windows 7 Live' licensed from versions of Detego Analyse v4.11 and above.

HOW TO USE THE TOOL

1. Create/license a field device from Detego Analyse. During the creation process, select the desired hashlists for the device.
2. Unzip the DetegoHashlistConverter.zip package onto the root of the newly created field device, e.g. as E:\DetegoHashlistConverter\
3. Run the DetegoHashlistConverter.exe, and a small dialog will appear.
4. Click 'Start' and wait for the process to complete; this could take some time for large hashlists.
5. Hashlists on the field device should now be visible/usable in both Config.exe (for Windows) and Config_Mac (for Mac) applications.

ADDITIONAL NOTES:

- Only MD5 hashes are supported for conversion to the legacy hashlists. This meets the Project VIC and CAID specification for minimally having MD5 hashes for all records.
- Legacy format hashlists do not support encryption. Therefore, this tool does not support field devices licensed with encrypted hashlists.

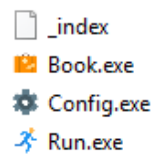
5.11. COVERT BOOKING PAGE

In a covert situation, the best option is often to configure in advance and run on the target. However, this is not always possible. In real-life situations, requirements can change, and there isn't time to go back and reconfigure the target machine. This is where the Covert Booking Page comes in. Designed to look like any other flight booking website, this tool allows you to create a new profile without raising suspicion that you're running extraction software on a computer. The options are more flexible in the full configuration tool, but you can still quickly enable/disable jobs from this tool.

STARTING THE TOOL

The Covert Booking Page is enabled by starting up a local webserver. This can be done by clicking on the shortcut Book.exe on the root of the Field Device.

Figure 299



STOPPING THE TOOL

You can close the webpage anytime and open it again by going to localhost: 8080. The underlying server will continue to be active until you quit it. To do this, navigate to the Contact tab.

Figure 300

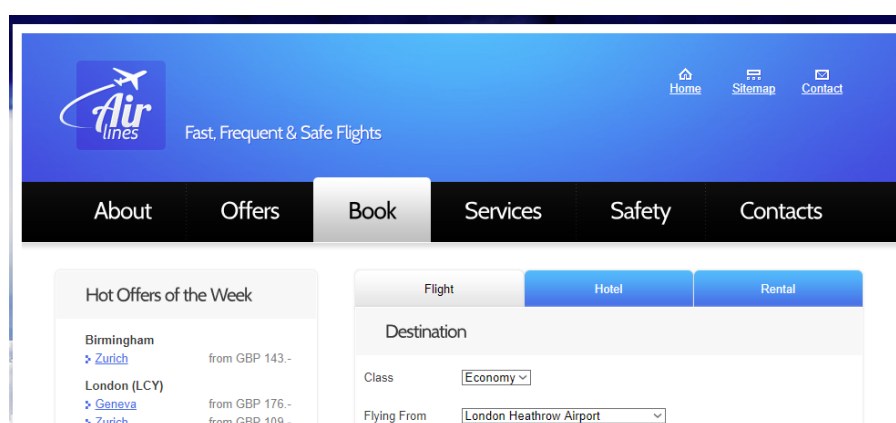


This will kill the server but won't stop any running extractions, so feel free to do it as soon as you are done configuring. To bring it back, you only need to run the Book.exe launcher again.

CONFIGURATION PAGE

The website mostly comprises generic pages that don't affect a Detego extraction. The tab to configure an extraction is the Book tab.

Figure 301



This page has various flight-themed options that are Detego Field options in disguise.

Once you fill out the full page and press Search for Flights, it will begin the extraction.

Seven types of jobs can be started with this tool.

The two that will always be run when using this tool are:

- Logical Extraction
- System Information

The five optional jobs are:

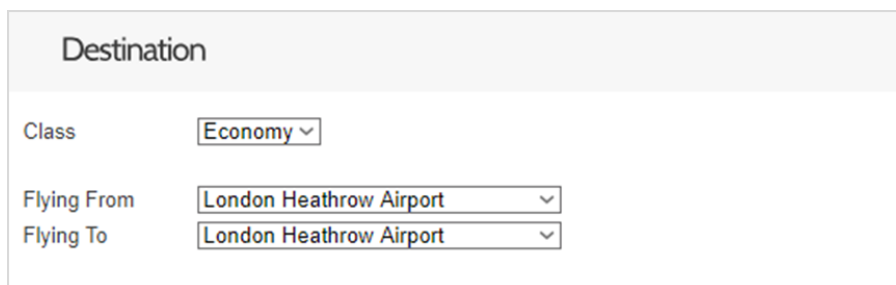
- Memory Extraction
- Internet Artefacts Extraction
- Physical Extraction
- Deleted Files Extraction
- Password Finder

LOGICAL JOB EXTRACTION

The first two sections of the Book page relate to the logical extraction of files.

- The Flying From and Flying To options will not affect the extraction; they are to make the page look more legitimate. The Class option allows you to choose how much of the target to extract from.
- The economy option will only extract files from the user directories on the machine—locations such as Desktop, Documents, and Downloads.
- The business option will extract files from the entire computer, including the user directories mentioned above.

Figure 302



The screenshot shows a form titled "Destination". It contains three rows of controls:

Destination	
Class	Economy
Flying From	London Heathrow Airport
Flying To	London Heathrow Airport

- The dates are the minimum and maximum time constraints for extracting files. If you were only interested in files from 6 to 3 months ago, you would set the two dates to those values.
- By leaving them both blank, there will be no time constraints.

Figure 303



The figure shows a light gray rectangular box with the title "Dates" in a bold, dark gray font. Below the title, there are two input fields. The first field is labeled "Out Date" in a dark gray font, and the second field is labeled "Return Date" in a dark gray font. Both fields are empty and have a thin black border.

ADDITIONAL CONFIGURATION

The Add-ons section allows you to turn on the other five jobs.

They are as follows:

- Memory Foam Pillow: Memory Extraction
- On Board Internet Access: Internet Artefacts Extraction
- Print Physical Copies of tickets: Physical Extraction
- Unallocated seating: Deleted (Unallocated) File Extraction
- Remember my Password: Password Extraction

Note: There is an extra option for **Overhead Storage**. This will turn on Header Checking for the Logical job if you want. This can cause the extraction to take longer, so leaving it off is recommended in time-sensitive situations.

RUNNING THE EXTRACTION

Once you've selected all your options, press the Search for Flights button, and your extraction will covertly begin. You can confirm the extraction has begun by checking that the icon has appeared in the system tray. Once you've confirmed Detego Field is running, you can safely close the webpage by navigating to the Contact tab to kill the server.

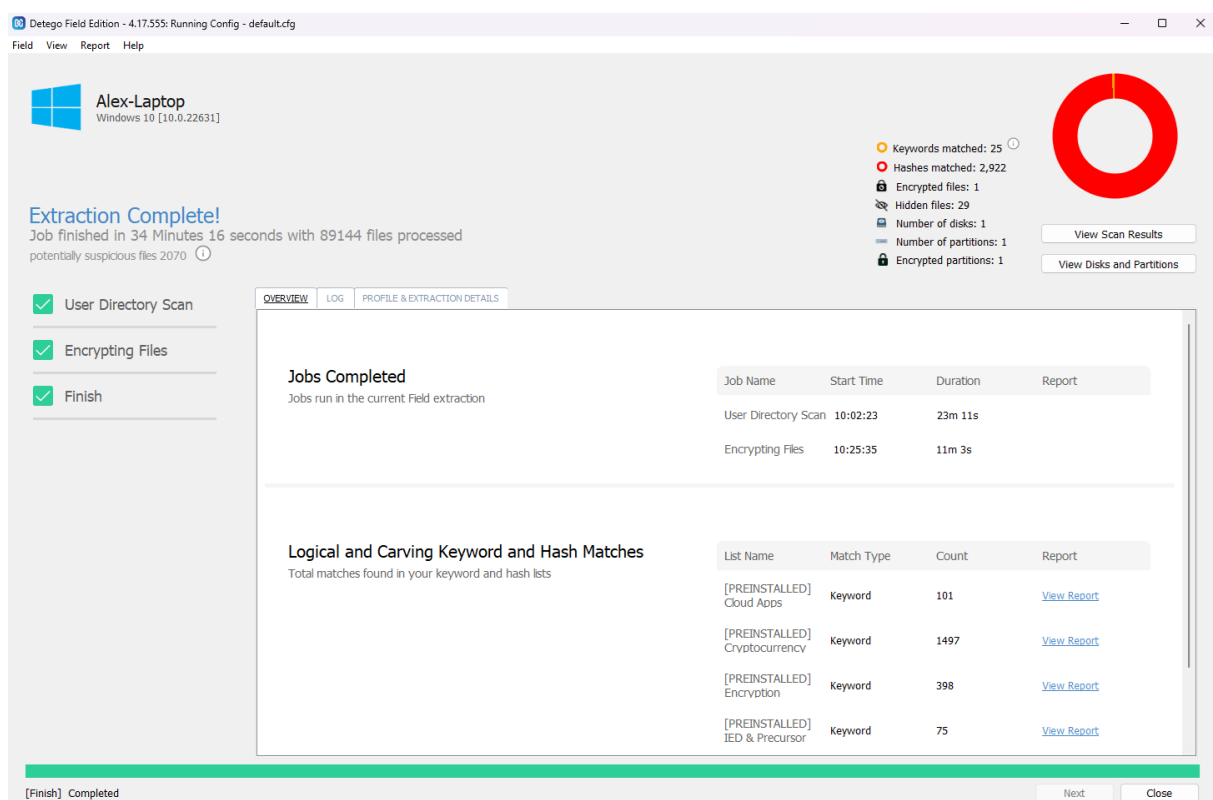
Figure 304

Search for Flights

5.12. DETEGO FIELD REPORTS

Once you've completed an extraction within Detego Field, specific jobs will have associated Detego Field Reports attached. From here, you can instantly see a report of all your results.

Figure 305



Clicking the 'View Report' button will display all extracted details and analytics completed, such as Hash Matching. These can all be viewed once a Field job has been completed.

The Hash Match report within Detego Field once complete does contain all details about the CAID/Project VIC Category that has been detected.

Figure 306

KeywordsAndHashMatches.html for exhibit 09-02-2024 16:46:46

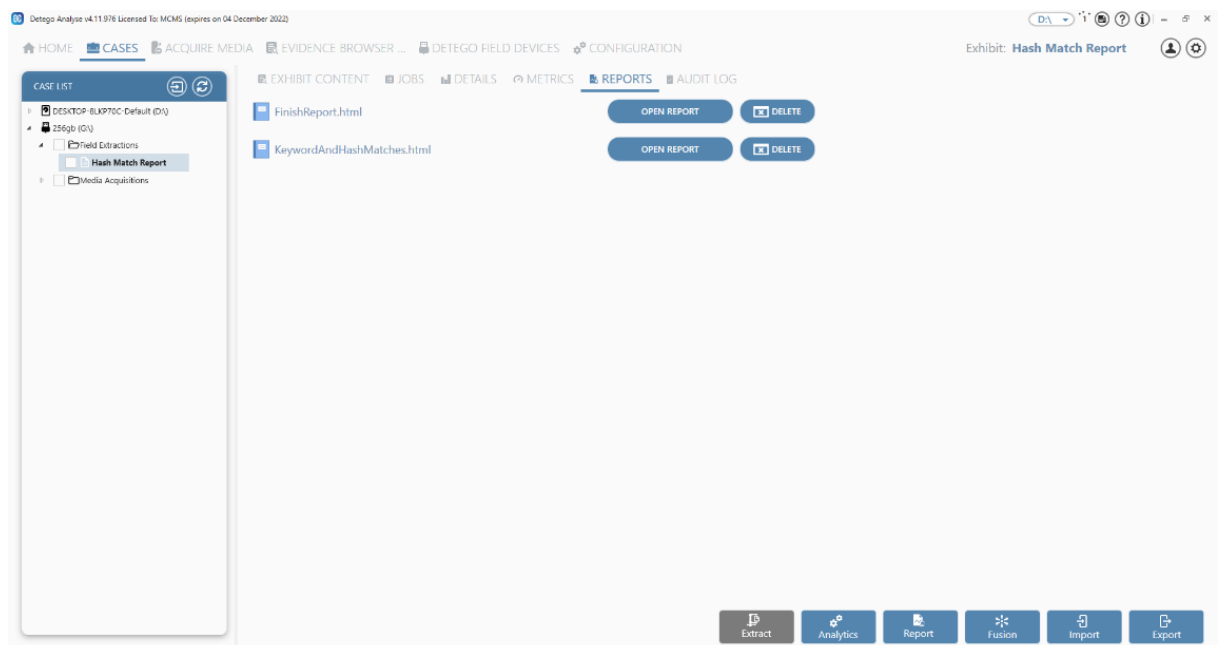
CAID_: OK (HASH-LOGICAL)

34 hashes matches with 90 hits

JOB LISTING	Hash Value	Hash Type	File Path
LOGICAL			
KEYWORD MATCH LISTS			
[PREINSTALLED] Cloud Apps	06d72035b50c0f9067a35b476e5b0e4	MD5	C:/Users/ThinkPad/Documents/PhotoDNA/190001.jpg
[PREINSTALLED] Cryptocurrency	06d72035b50c0f9067a35b476e5b0e4	MD5	C:/Users/ThinkPad/Documents/PhotoDNA/190001.jpg
[PREINSTALLED] Encryption	06d72035b50c0f9067a35b476e5b0e4	MD5	C:/Users/ThinkPad/Documents/PhotoDNA/190001.jpg
HASH MATCH LISTS			
CAID 1 (List)			
Extreme Pornography	896b5ef5dd16bb6f54e9073204f6b31	MD5	C:/Users/ThinkPad/Documents/PhotoDNA/190011.jpg
Hash Match	896b5ef5dd16bb6f54e9073204f6b31	MD5	C:/Users/ThinkPad/Documents/PhotoDNA/190011.jpg
Indicative / Borderline	14e655ef912432ba3a64b14b4848ffa	MD5	C:/Users/ThinkPad/Documents/PhotoDNA/190027.jpg
Prohibited Images of Children	14e655ef912432ba3a64b14b4848ffa	MD5	C:/Users/ThinkPad/Documents/PhotoDNA/190027.jpg
SC Category A	1d5815a07401636b49e39f56f0ba10d1	MD5	C:/Users/ThinkPad/Documents/Test_data_1k190027.jpg
SC Category B	1d5815a07401636b49e39f56f0ba10d1	MD5	C:/Users/ThinkPad/Documents/Test_data_1k190027.jpg
SC Category C	1d5815a07401636b49e39f56f0ba10d1	MD5	C:/Users/ThinkPad/Documents/Test_data_1k190027.jpg
Unconfirmed	b7e1f90cd4eba3e1eeaa26fa07844613	MD5	C:/Users/ThinkPad/Documents/PhotoDNA/190031.jpg
CAID III (List)			
IKKE relevant (for saken)	b7e1f90cd4eba3e1eeaa26fa07844613	MD5	C:/Users/ThinkPad/Documents/PhotoDNA/190031.jpg
CAID_ (List)			
???	c54eca35e45d5a1379c0da1ae0e0e6	MD5	C:/Users/ThinkPad/Documents/Test_data_1k190031.jpg
Child abuse content	c54eca35e45d5a1379c0da1ae0e0e6	MD5	C:/Users/ThinkPad/Documents/PhotoDNA/190032.jpg
Extreme Child abuse	c54eca35e45d5a1379c0da1ae0e0e6	MD5	C:/Users/ThinkPad/Documents/Test_data_1k190032.jpg
Hash Match	61e83a5ac19d40ed73567ced1321fcac	MD5	C:/Users/ThinkPad/Documents/PhotoDNA/190034.jpg
OK	61e83a5ac19d40ed73567ced1321fcac	MD5	C:/Users/ThinkPad/Documents/PhotoDNA/190034.jpg
Possible new victim (CP)	61e83a5ac19d40ed73567ced1321fcac	MD5	C:/Users/ThinkPad/Documents/Test_data_1k190034.jpg
Unknown	7d57e1b54562b4453b62b6cea0d6db7	MD5	C:/Users/ThinkPad/Documents/PhotoDNA/190056.jpg
ebooks_MD5 (List)	7d57e1b54562b4453b62b6cea0d6db7	MD5	C:/Users/ThinkPad/Documents/PhotoDNA/190056.jpg
Hash Match	7d57e1b54562b4453b62b6cea0d6db7	MD5	C:/Users/ThinkPad/Documents/Test_data_1k190056.jpg
	0389ac755287ecc8427f497cfab5a12e	MD5	C:/Users/ThinkPad/Documents/PhotoDNA/190086.jpg
	0389ac755287ecc8427f497cfab5a12e	MD5	C:/Users/ThinkPad/Documents/PhotoDNA/190086.jpg
	0389ac755287ecc8427f497cfab5a12e	MD5	C:/Users/ThinkPad/Documents/PhotoDNA/190086.jpg
	e1542e6fa024c2c759eb65851d9bd99	MD5	C:/Users/ThinkPad/Documents/PhotoDNA/190099.jpg
	e1542e6fa024c2c759eb65851d9bd99	MD5	C:/Users/ThinkPad/Documents/PhotoDNA/190099.jpg
	9fa899f33b39d33958da03e77ca477da	MD5	C:/Users/ThinkPad/Documents/Test_data_1k190099.jpg
	9fa899f33b39d33958da03e77ca477da	MD5	C:/Users/ThinkPad/Documents/PhotoDNA/190101.jpg
	9fa899f33b39d33958da03e77ca477da	MD5	C:/Users/ThinkPad/Documents/PhotoDNA/190101.jpg
	9fa899f33b39d33958da03e77ca477da	MD5	C:/Users/ThinkPad/Documents/Test_data_1k190101.jpg
	50201b60b6b6e4815a4adb1a78ac0cd	MD5	C:/Users/ThinkPad/Documents/PhotoDNA/190124.jpg

When you import your Field Extractions, these will automatically be imported into Detego Analyse. These are under the 'Reports' Tab within your Detego Analyse Exhibit.

Figure 307



5.13. IMPORTING DETEGO FIELD/BALLISTIC

Once you have completed Detego Field Extractions or Ballistic Extractions, you must import them into Detego Analyse for further Analytics and post-processing.

IMPORTING A FIELD EXTRACTION

To import a Field Extraction, follow the below steps:

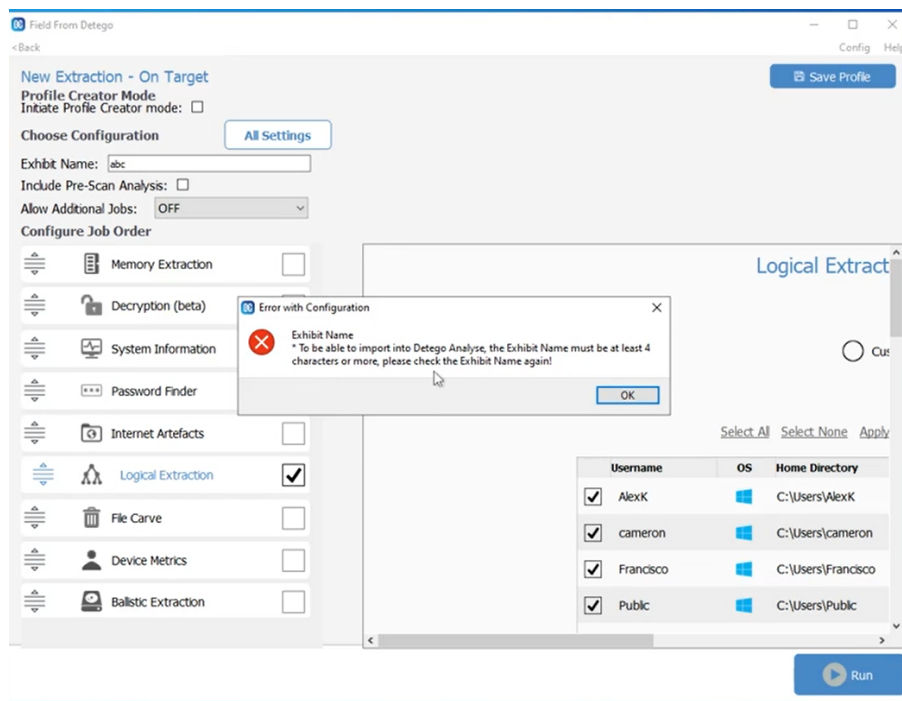
- From the Detego Analyse home screen, insert your Field Device into your Detego Analyse machine.
- Detego should recognise the Field Device connected, and a 'Detego® Device Detected' prompt will display. Select the **IMPORT** button.

Figure 308



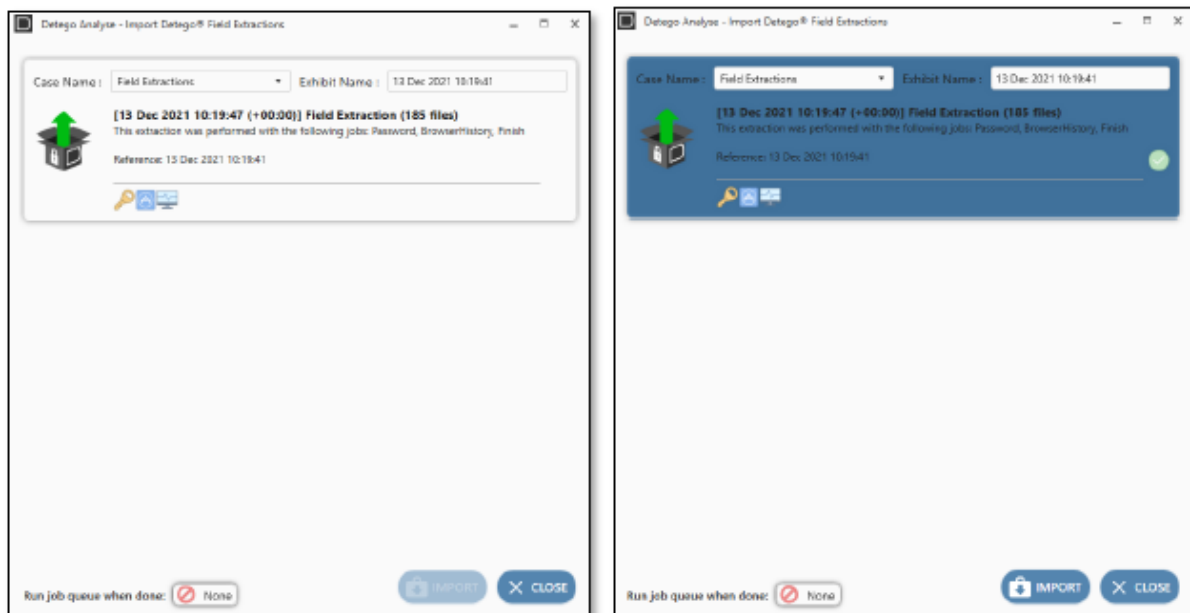
- After selecting the IMPORT button, the 'Import Detego Field Extractions' window will display. You can select the Extractions you wish to import into Detego Analyse.
- When importing Detego Field extractions, the import window shows the profile name used on-target. This information is stored in the Exhibit Metadata and is visible on the Exhibit Properties window after import.
- You can also select the 'Case Name' dropdown to choose a case to save the extraction to or type in a name for the case that will create a new case with that name. You can type in the 'Exhibit Name' box to change the exhibit's name. The naming convention will follow the standard 'Exhibit Names' principles.

Figure 309



- You can also use the 'Run job queue when done!' button to run a job queue once the import has been completed.

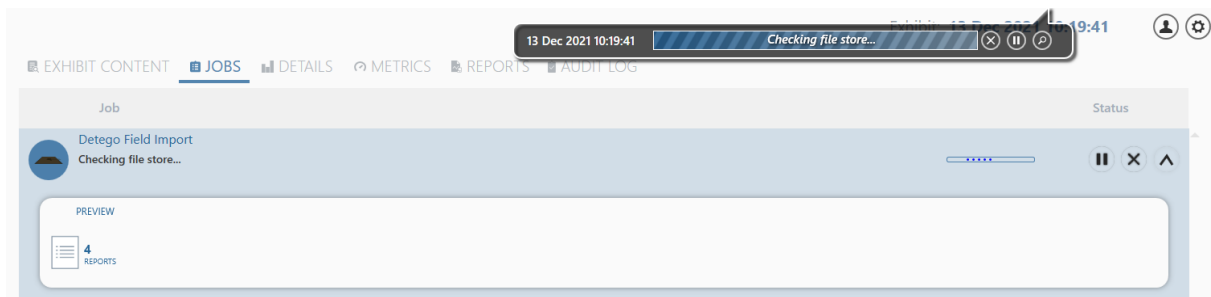
Figure 310



- Once you are happy with your selection, select the IMPORT button to start the Field import job. After selecting an extraction, you'll also notice that extraction will display blue with a green tick on the side, and the IMPORT button will be available.

- You will then be taken to the JOBS tab in Cases to see the progress of the import job.

Figure 311



- Alternatively, you can click the IMPORT button from the Field device inserted within the 'Field Devices' tile from the home screen. This will open the same IMPORT window as the previous steps.

Figure 312

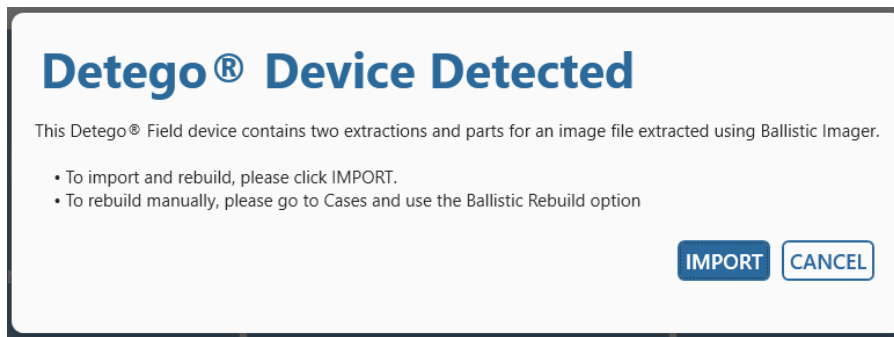


REBUILDING A BALLISTIC IMAGE

To import and rebuild a Ballistic Extraction, follow the below steps:

- From the Detego Analyse home screen, insert your Ballistic Device into your Detego Analyse machine.
- Detego should recognise the Ballistic Device connected, and a 'Detego® Device Detected' prompt will display. Select the **IMPORT** button.

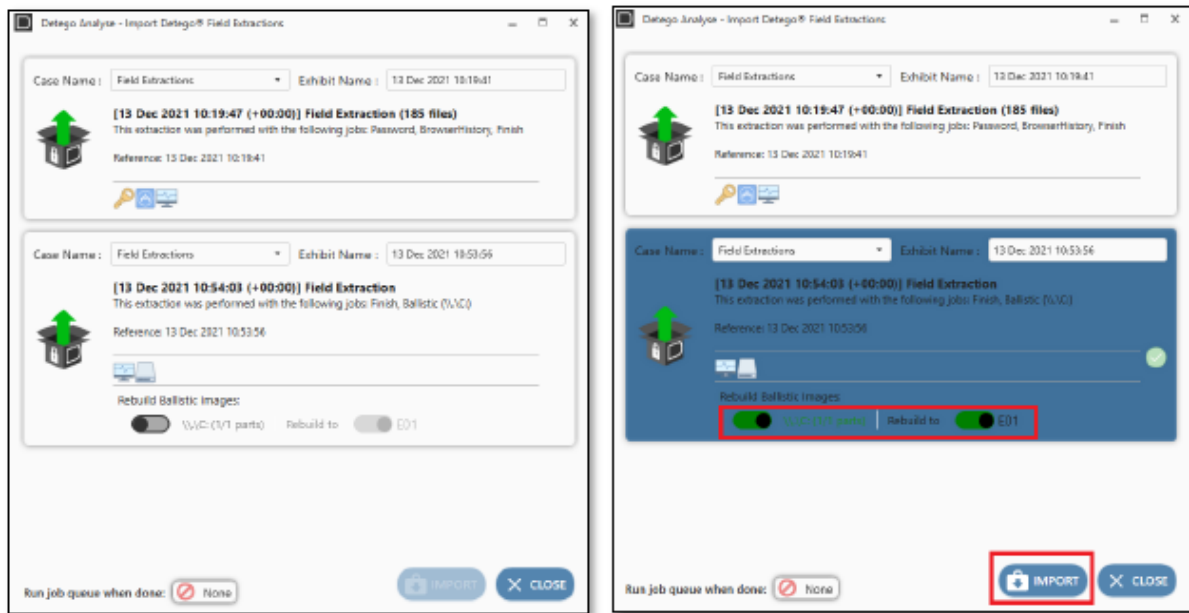
Figure 313



- After selecting the IMPORT button, the 'Import Detego Field Extractions' window will display. You can select the Ballistic extraction you wish to import and rebuild into Detego Analyse.
- You can also select the 'Case Name' dropdown to choose a case to save the extraction to or type in a name for the case that will create a new case with that name. You can type in the 'Exhibit Name' box to change the exhibit's name.
 - **NOTE.** If you try to rebuild an image which is too large for the storage volume, a warning will appear. If the image is rebuilt to an E01 file, you will be warned but still allowed to proceed if you wish.
- You can also use the 'Run job queue when done:' button to run a job queue once the import has been completed.

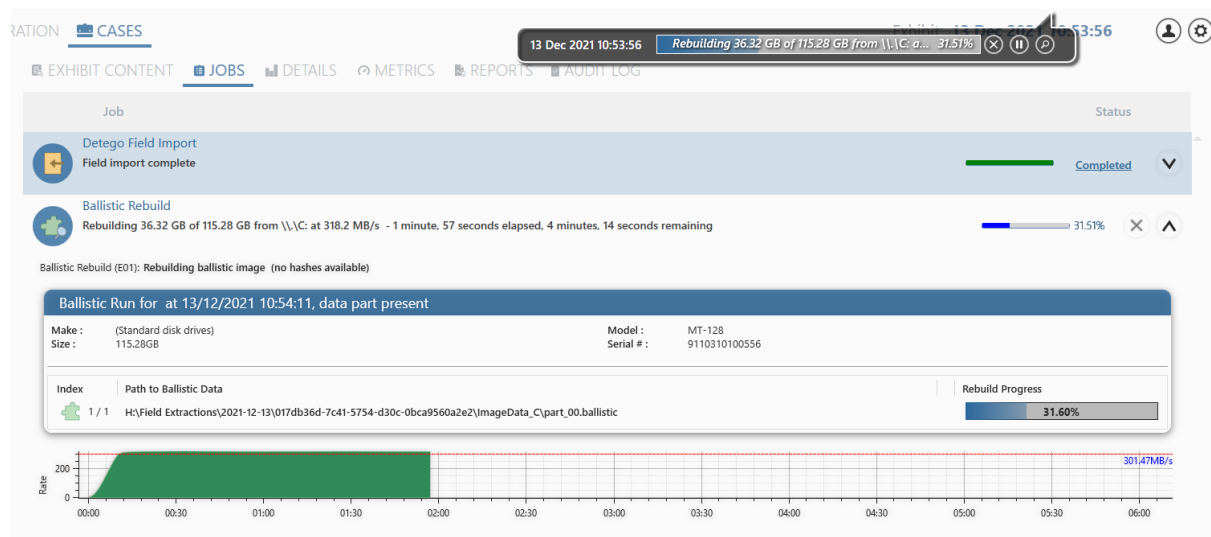
WARNING! TO REBUILD THE EXTRACTION INTO AN IMAGE FORMAT, you MUST select the 'Rebuild Ballistic images:' toggle button to REBUILD THE EXTRACTION INTO AN IMAGE FORMAT. The toggle next to it allows you to select the format (either E01 or DD).

Figure 314



- Once you are happy with your selection, select the IMPORT button to start the Field import job. After selecting an extraction, you'll also notice that extraction will display blue with a green tick on the side, and the IMPORT button will be available.
- You will then be taken to the JOBS tab in Cases to see the progress of the import job.

Figure 315



- Alternatively, you can select the IMPORT button from the Field device inserted within the 'Field Devices' tile from the home screen. This will open the same IMPORT window as the previous steps.

Figure 316

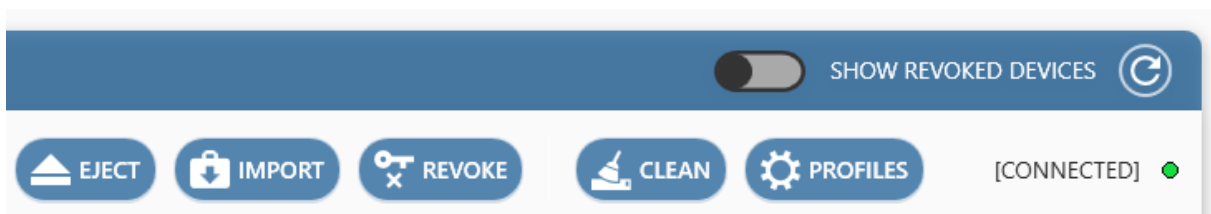


5.14. CLEANING AND REVOKING FIELD DEVICES

This section will cover cleaning and revoking your Field devices.

WARNING! Please import any Field Extractions or Ballistic Images before cleaning or revoking; otherwise, you may lose all extracted data.

Figure 317



CLEANING FIELD DEVICES

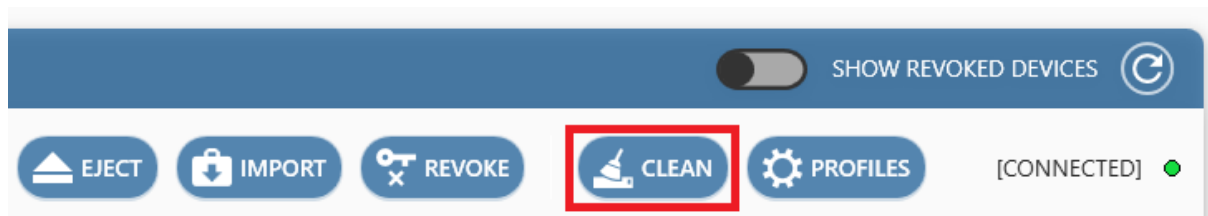
Cleaning a Field device allows you to clear any Field extractions from the device, making it possible to run more Field extractions. This is useful if you only have one device and limited space on the device and need to clear some space to allow another extraction.

Please import any extractions before cleaning a device to prevent data loss.

To clean a device, follow the below steps:

- Insert the Field device you wish to clean of extractions.
- Select the 'CLEAN' button on the Field device you wish to clean from the Field Devices window.

Figure 318



- From the confirmation prompt that appears, select YES to confirm the operation. This will clean the extractions from the device. Select NO if you wish to cancel the operation.

REVOKING FIELD DEVICES

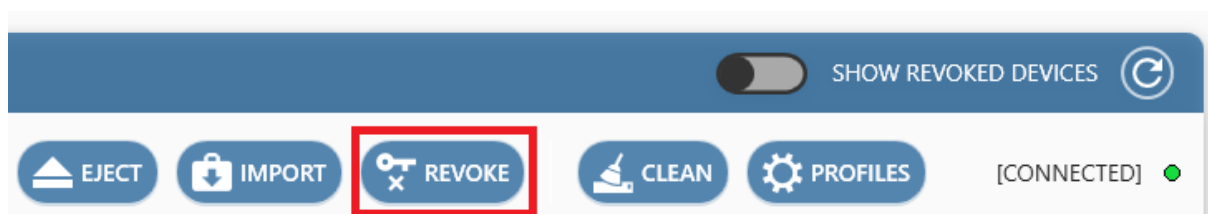
Revoking a Field device clears it and reformats it back to exFAT format. This allows you to clean down any of its data, remove old boot partitions and remove it as a Field device. You can then use the device as a storage device for something else or relicense it as a Field device if you wish.

NOTE! To prevent data issues and loss, you must import and revoke a Field device before upgrading any Detego installation.

To revoke a Field Device, follow the steps below:

- Insert your Field device into your machine
- Select the 'Field Devices' tile
- On your chosen Field device, select the 'REVOKE' button.

Figure 319



- The below pop-up window will appear asking you to confirm the revoking of the device:

Figure 320



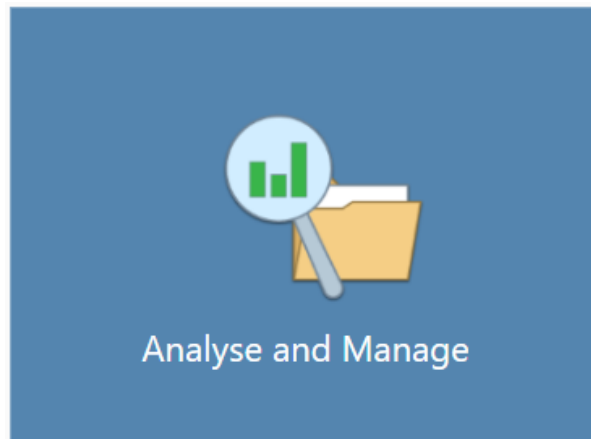
There are two [2] possible toggle options that will appear:

1. **Securely Erase Detego® Field Data on Revoke** – When switched on, this will perform an extensive Diskpart clean wipe (The most secure way of formatting a device). If switched off (default), it will perform a regular Windows device format. Toggling this on will significantly increase the time to revoke a device.
 2. **'Remove Detego® Boot Environment on Revoke** – When switched on, this will format and remove any boot partitions you may find on the device if it was licensed with the boot environment on it. (This option is only displayed if the device has boot partitions).
- You can select CONFIRM to revoke the device or CANCEL to cancel the process from this screen. The device will appear in the 'Show Revoked Devices' window and be available for relicensing.

6. ANALYSE AND MANAGE

The 'Analyse and Manage' module lets you view, edit, export, delete, and run analytics for cases and exhibits. Although exhibits from Media Acquisition can be viewed instantly, those acquired by Field Extraction only become viewable once the data has been imported from the Field device into Detego Analyse.

Figure 321



From here, you can also conduct analytical processes including but not limited to:

- Keyword Matching
- Hash Matching
- Text Indexer
- Picture and Video Analytics
- EXIF Processor
- Compound File Extractor
- Drone Parser

And many more.

6.1. CASE MANAGEMENT

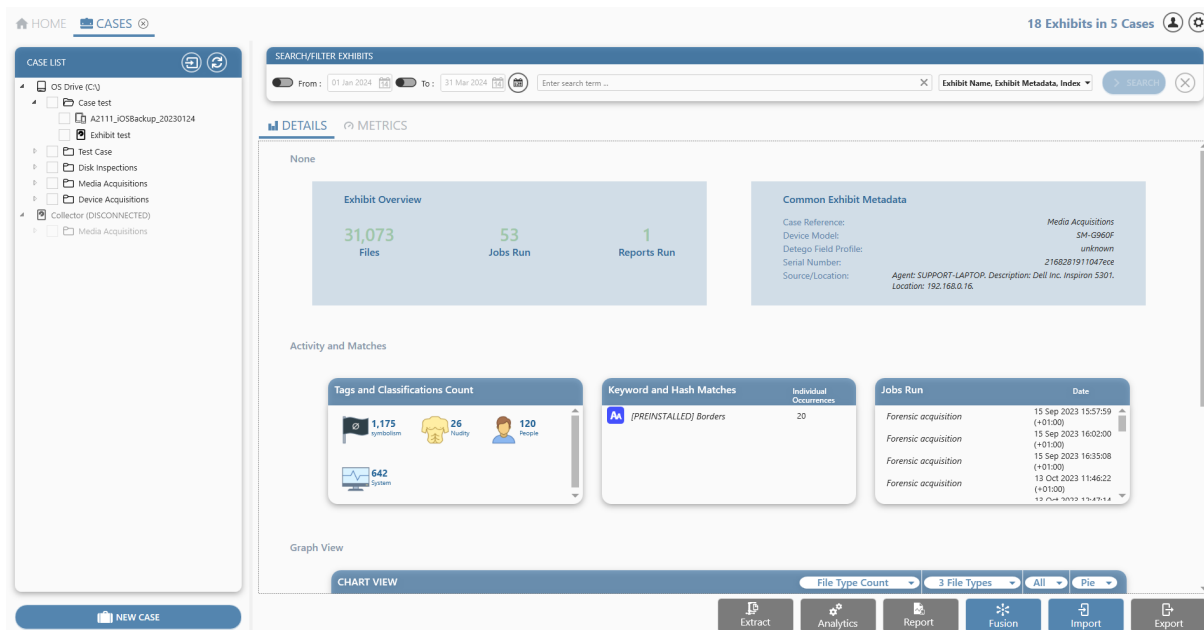
This section will guide you in managing your cases and exhibits including creating, moving and deleting as well as other actions.

THE CASE MANAGEMENT HOME SCREEN

The Case Management Home Screen will look like the below image or similar (may vary depending on cases and exhibits you already have on your instance).

By default, cases are identified within the Case List, separated by the date and type of acquisition, and exhibits by timestamp; however, you can edit this metadata inside the module or during extraction.

Figure 322



SEARCH/FILTER EXHIBITS

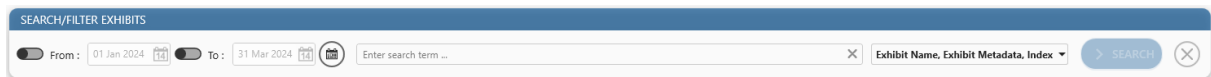
If you have selected a Case from your Case List rather than an exhibit, the Search/Filter Exhibits bar will be displayed above Details and Metrics sections allowing you to search the case for specific exhibits, items and files.

- The 'From' and 'To' boxes allow you to select a date to search from and to. (e.g., From 18/01/2012 – 18/01/2013 will search within that date range.)

- The longest box here allows you to type your search term in.
- The 'Exhibit Name...' dropdown allows you to select what you are searching for. These include searching everything and Searching exhibit properties.

Once you have selected your search criteria, select the SEARCH button to complete the search.

Figure 323



ACTION BUTTONS

The Action Buttons allow for various functionality with fewer clicks. The Action buttons available are:

- **Extract** - This allows you to start an extraction directly from the selected case.
- **Analytics** - This allows you to start an Analytical job or run a job queue from one of your extractions within a case.
- **Fusion** - allows you to use the link-building functionality to uncover connections between exhibits.
- **Report** - This allows you to create a report for your selected exhibit.
- **Import** - This allows you to import data into your exhibit or case.
- **Export** - This allows you to export an exhibit or data.

Figure 324

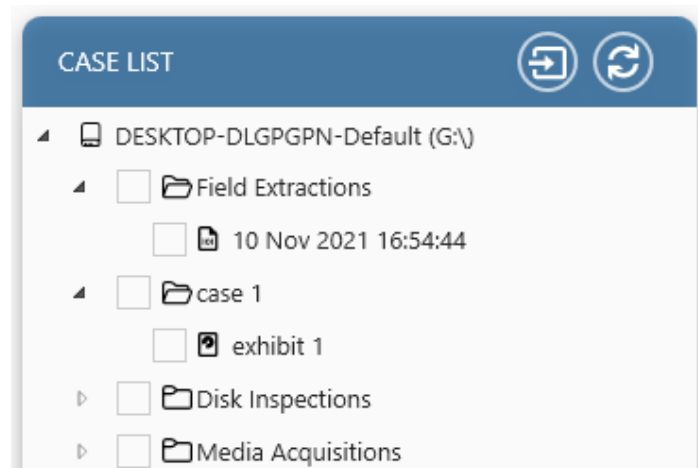


Please note that depending on the case, exhibit and data you already have, one or more of these Action buttons may be greyed out.

CASE LIST

The Case List will be displayed on the left side panel. From here, you can select the storage device, case and exhibit.

Figure 325



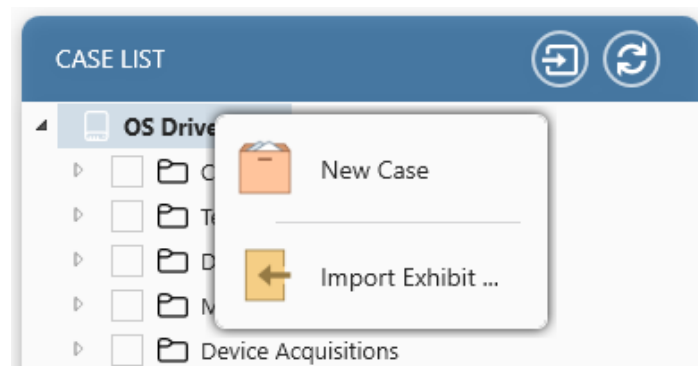
- Selecting the small dropdown arrow will expand or collapse the case and display any created exhibits.
- The Storage Volume drive is typically the parent in the tree, Cases being the folders within and then Exhibits being the items within those folders.
- Right clicking on a Storage Volume, Case or Exhibit will provide you with various options allowing for actions to perform.

STORAGE VOLUME OPTIONS

A Storage Volume contains your Cases. Below is a list of available options from the Storage Volume context menu within the Case List; further details can be found later in this guide:

- **New Case**
- **Import Exhibit ...**

Figure 326



CASE OPTIONS

A Case contains your Exhibits and is nested inside a Storage Volume. Below is a list of available options from the Case context menu within the Case List; further details can be found later in this guide:

- **New Case**
- **New Exhibit**
- **Detego Ballistic Rebuild**
- **Artefact_Compare**
- **Delete Case**
- **Import Exhibit ...**
- **Case Metadata ...**

Figure 327

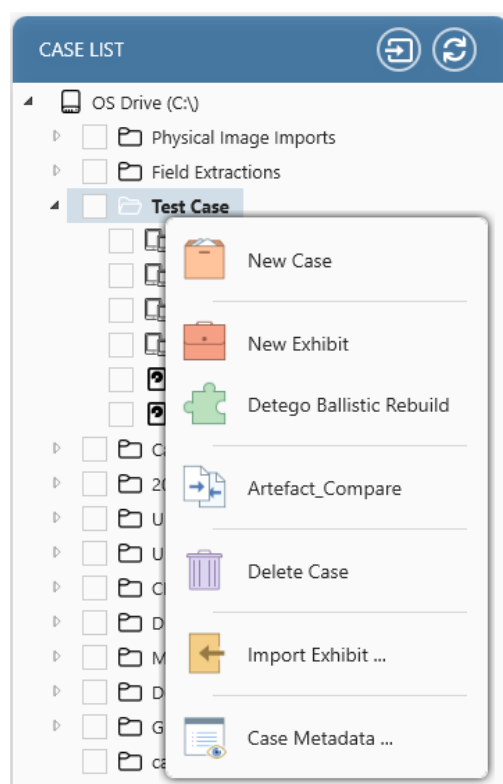


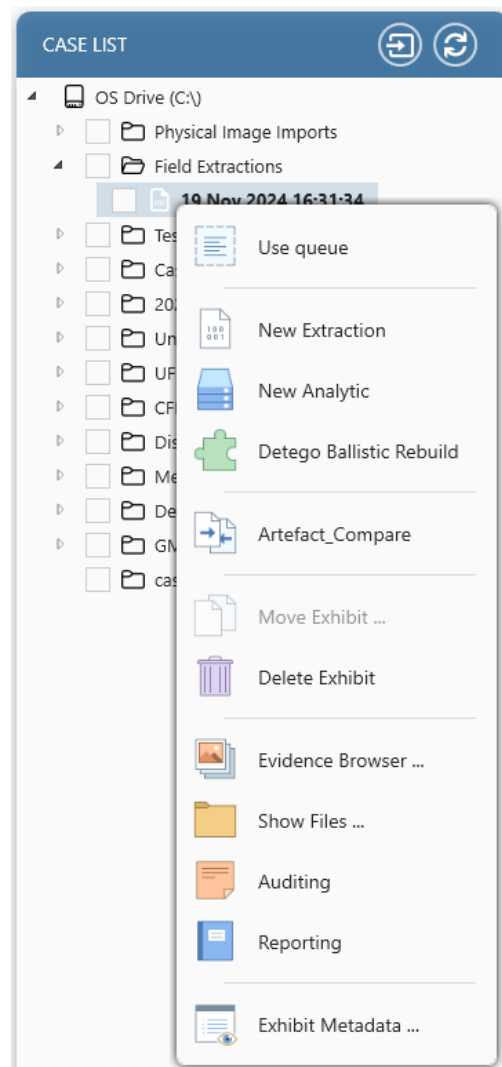
EXHIBIT OPTIONS

An Exhibit contains your data and is nested inside a Case. Below is a list of available options from the Exhibit context menu within the Case List; further details can be found later in this guide:

- **Use queue >**
- **New Extraction**
- **New Analytic**
- **Detego Ballistic Rebuild**
- **Artefact_Compare**
- **Move Exhibit ...**
- **Delete Exhibit**
- **Evidence Browser ...**

- **Show Files ...**
- **Auditing**
- **Reporting**
- **Exhibit Metadata ...**

Figure 328

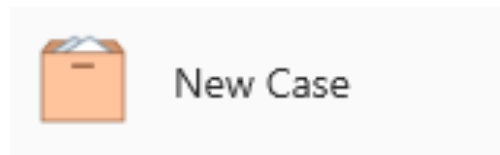


NEW CASE

To create a New Case, follow the below steps:

- Right click a Storage Volume or Case from the Case List
- Select the 'New Case' option from the menu

Figure 329



- Alternatively, if you have a Storage Volume selected within your Case List, then you will see the big 'NEW CASE' button at the bottom of the Case List:

Figure 330



The below screen will display after selecting the 'New Case' option or button:

Figure 331

A screenshot of a web application window titled "Detego Analyse - New Case". The window contains several input fields: "Case reference:" (highlighted in pink), "Suspect name:", "Start date:" (with a date picker showing "26 Feb 2024 11:49:42"), "Notes:" (a large text area), and "Examiner:". At the bottom left, a red error message reads "A value is required for 'Case Reference'". At the bottom right, there are two buttons: "NEW CASE" and "CANCEL".

- Fill out the Case metadata for your New Case.
 - Case reference - This is the name of the Case. (This is a required field)
 - Suspect name - This is the name of the suspect for the Case.
 - Start date - The start date of the Case.
 - Notes - Any notes about the Case you wish to include.

- Examiner - The examiner for the Case.
- Once you are happy with the Case details, select the 'NEW CASE' button at the bottom right corner of the New Case window to create the Case.

CASE METADATA

Case Metadata can be filled out when creating a Case; however, you are able to edit the Case Metadata at any time.

To edit the Metadata of a Case, follow the below steps:

- From the Case List, right click on the Case you wish to edit the Metadata of.
- Select the 'Case Metadata' option.

Figure 332



- From this 'Edit Metadata...' window, you can edit any of the information contained here.

Figure 333

 A screenshot of a web application window titled 'Detego Analyse - Edit Metadata for case 'Case test''. The window contains several input fields: 'Case reference:' with the value 'Case test', 'Suspect name:' (empty), 'Start date:' with the value '15 Sep 2023 15:54:04' and a calendar icon, 'Notes:' (empty), and 'Examiner:' (empty). At the bottom right, there are two buttons: 'UPDATE CASE' with a list icon and 'CANCEL' with an 'X' icon.

- Once you have made your changes, select the 'UPDATE CASE' button in the bottom right corner.

DELETE CASE

There are two methods of deleting a Case from your Case List.

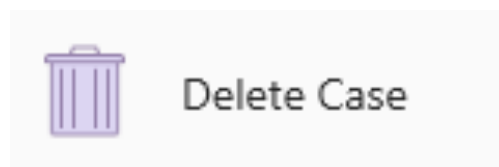
Please be aware that any exhibits within the Case(s) will be permanently deleted and you will lose any and all data from the deleted exhibits. Remember to back-up any important data and exhibits before deleting.

DELETING A SINGLE CASE

In order to delete a single Case, follow the below steps:

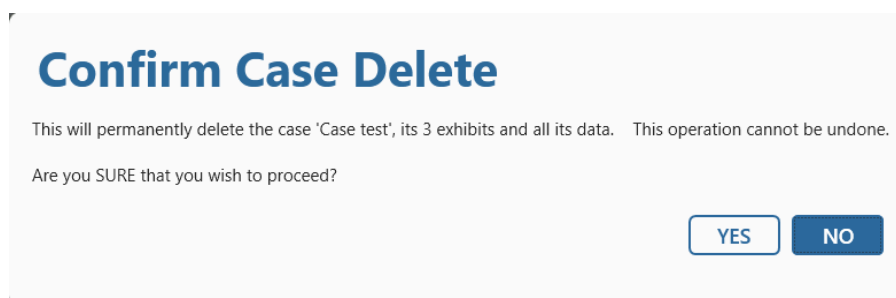
- From the Case List, right click on the case you wish delete.
- Select the 'Delete Case' option from the right click menu.

Figure 334



- If you are happy to delete, select 'YES' when prompted to delete the Case.

Figure 335

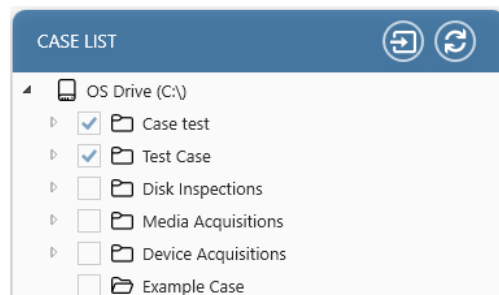


DELETING MULTIPLE CASES

In order to delete multiple Cases, follow the below steps:

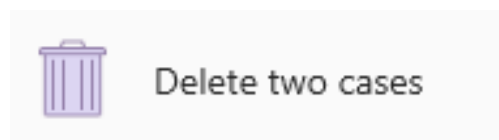
- From the Case List, select the checkbox on the Cases you wish to delete.

Figure 336



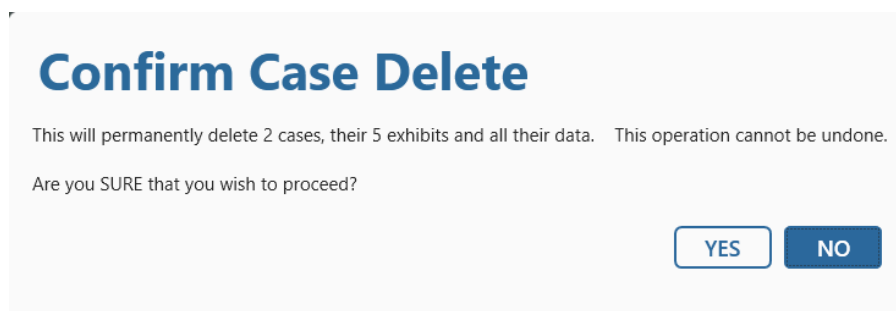
- Once the Cases are selected, right click on one of the selected Cases.
- Select 'Delete X cases' where X represents the number of Cases you have selected.

Figure 337



- When prompted with a Confirmation on deleting the selected Cases, select YES.

Figure 338



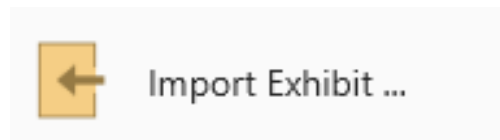
IMPORT EXHIBIT

You can import an Exhibit into an existing Case or Storage Volume.

To do this follow the below steps:

- From the Case List, right click on a Case or Storage Volume.
- Select the 'Import Exhibit ...' option.

Figure 339



This will then open the Import window. For more information, please navigate to Importing Exhibits section within this guide.

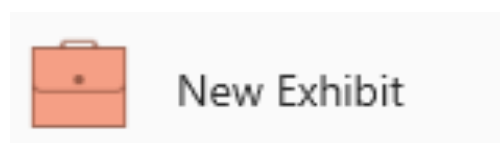
NEW EXHIBIT

Exhibits can be created manually or automatically depending on your process.

In order to manually create a New Exhibit, please follow the below steps:

- From your Case List, right click on the Case you wish to create an Exhibit under.
- Select the 'New Exhibit' option.

Figure 340



- This will open up the 'New Exhibit...' window.

Figure 341

A screenshot of a web application window titled 'Detego Analyse - New Exhibit in case 'Case test''. The form contains several input fields: 'Storage volume' (a dropdown menu showing 'OS Drive OS' and '569.4 GB free'), 'Exhibit reference' (a red highlighted field with a red error message 'A value is required for 'Exhibit Reference'' at the bottom left), 'Description', 'Serial number', 'Device model', 'Notes' (a large text area), 'Source/Location', and 'Time zone' (a dropdown menu showing '(UTC+00:00) Dublin, Edinburgh, Lisbon, London'). On the right side of the form, there is a vertical scrollbar and a '+' icon. At the bottom right, there are two buttons: 'NEW EXHIBIT' and 'CANCEL'.

- Fill in the details of your new Exhibit.
 - **Storage Volume** - This Dropdown allows you to select the Storage Volume to save the Exhibit.
 - **Exhibit reference** - This is the name of the Exhibit. (This field is required)
 - **Description** - This is the description of the Exhibit.
 - **Serial Number** - This is the serial number of the device (if applicable).
 - **Device model** - This is the mode of the device (if applicable).
 - **Notes** - This is for any notes you wish to include with your Exhibit.
 - **Source/Location** - This is the source or location the device was acquired.
 - **Time zone** - This dropdown allows you to select the time zone for the Exhibit.
 - **The Camera icon** - This allows you to take a picture for the Exhibit to add to the Metadata.
 - **The + button** - This button allows you to attach images/pictures to the Exhibit Metadata which can be viewed in the DETAILS tab.
- When you have filled in the Exhibit Metadata with the details, select the 'NEW EXHIBIT' button in the bottom right corner of the window.

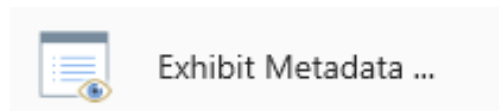
EXHIBIT METADATA

Exhibits Metadata can be edited after the Exhibit has been created, allowing you to be more specific with what the Exhibit is/contains.

To edit the Exhibit Metadata, please follow the below steps:

- From your Case List, right click on the Exhibit you wish to edit the Metadata of.
- Select the 'Exhibit Metadata ...' option.

Figure 342



- This will open up the 'Edit Metadata ...' window.

Figure 343

A screenshot of the 'Detego Analyse - Edit Metadata for exhibit 'Exhibit test' in case 'Case test' window. The window contains several input fields: 'Storage volume' (OS Drive OS, 569.4 GB free), 'Exhibit reference' (Exhibit test), 'Description', 'Serial number', 'Device model', 'Notes', 'Source/Location', and 'Time zone' (UTC+00:00) Dublin, Edinburgh, Lisbon, London). At the bottom right are 'UPDATE EXHIBIT' and 'CANCEL' buttons.

- Fill in the details to edit your Exhibit Metadata.
 - **Storage Volume** - This Dropdown allows you to select the Storage Volume to save the Exhibit. (You cannot move an Exhibit to another location using this option).
 - **Exhibit reference** - This is the name of the Exhibit. (This field is required)
 - **Description** - This is the description of the Exhibit.
 - **Serial Number** - This is the serial number of the device (if applicable).
 - **Device model** - This is the mode of the device (if applicable).
 - **Notes** - This is for any notes you wish to include with your Exhibit.
 - **Source/Location** - This is the source or location the device was acquired.

- **Time zone** - This dropdown allows you to select the time zone for the Exhibit.
- **The Camera icon** - This allows you to take a picture for the Exhibit to add to the Metadata.
- **The + button** - This button allows you to attach images/pictures to the Exhibit Metadata which can be viewed in the DETAILS tab.
- When you have filled in the Exhibit Metadata with the details, select the 'UPDATE EXHIBIT' button in the bottom right corner of the window.

MOVE EXHIBIT

There are a few methods of moving Exhibits. You can move a single Exhibit or multiple Exhibits.

MOVING EXHIBITS - DRAG AND DROP

When you are moving Exhibits within a Storage Volume or to another Storage Volume, you can select it and drag and drop it into another Case.

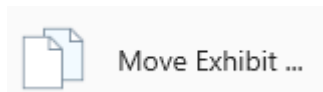
Currently this method is not supported for multiple Exhibits at once.

MOVING EXHIBITS - RIGHT CLICK

When you are you are moving Exhibits to another Storage Volume, follow the below steps:

- Right click on the Exhibit you wish to move
- Select the 'Move Exhibit ...' option.

Figure 344



- From the 'Switch Exhibit Volume' prompt, select the Storage Volume you wish to move the Exhibit to from the Dropdown list. (You will need to have at least 1 other Storage Volume added within Configuration to allow this to work.)

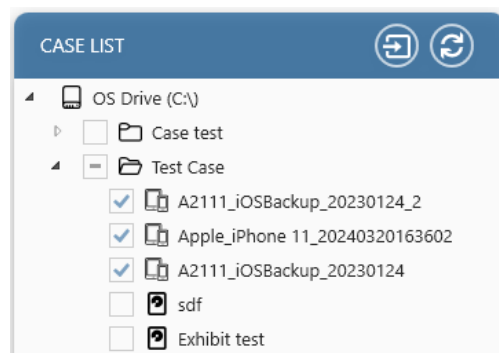
Figure 345



You can also check do the same for multiple Exhibits:

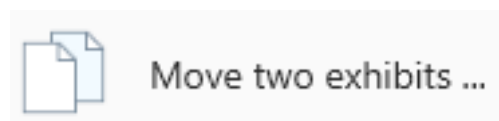
- From the Case List, check the tickboxes of the Exhibits you wish to move.

Figure 346



- Right click on one of the checked Exhibits.
- Select the 'Move X exhibits ...' option.

Figure 347



This will then display the above mentioned 'Switch Exhibit Volume' Prompt where you can select the Storage Volume you wish to move the Exhibits to.

DELETE EXHIBIT

There are two methods of deleting an Exhibit from your Case List.

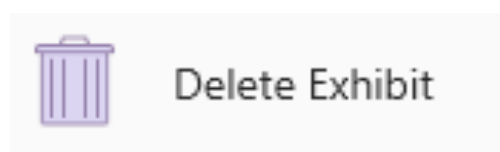
Please be aware that any and all data within an exhibit will be permanently deleted. Remember to back-up any important data and exhibits before deleting.

DELETING A SINGLE EXHIBIT

In order to delete a single Exhibit, follow the below steps:

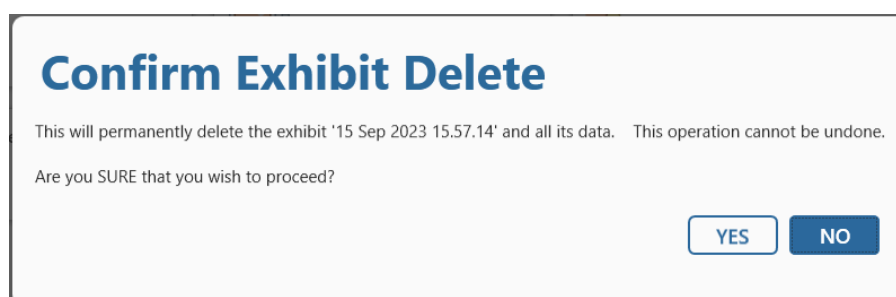
- From the Case List, right click on the exhibit you wish delete.
- Select the 'Delete Exhibit' option from the right click menu.

Figure 348



- If you are happy to delete, select 'YES' when prompted to delete the Exhibit.

Figure 349

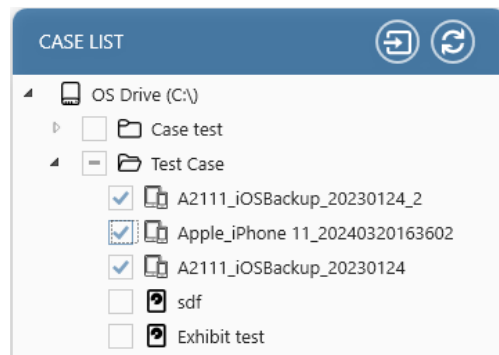


DELETING MULTIPLE EXHIBITS

In order to delete multiple Exhibits, follow the below steps:

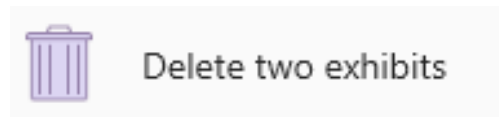
- From the Case List, select the checkbox on the Exhibits you wish to delete.

Figure 350



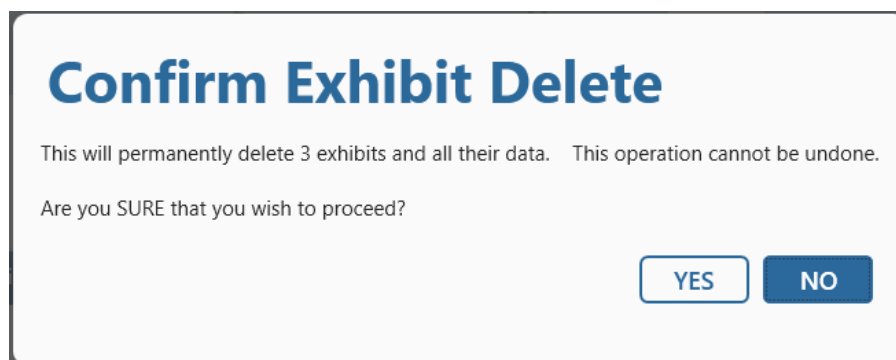
- Once the Exhibits are selected, right click on one of the selected Exhibits.
- Select 'Delete X exhibits' where X represents the number of Cases you have selected.

Figure 351



- When prompted with a Confirmation on deleting the selected Exhibits, select YES.

Figure 352

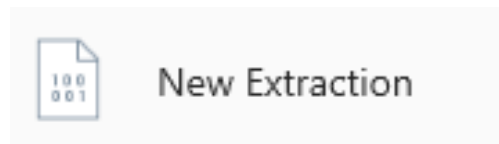


NEW EXTRACTION

From the Case List, you can start a New Extraction. To do this, follow the below steps:

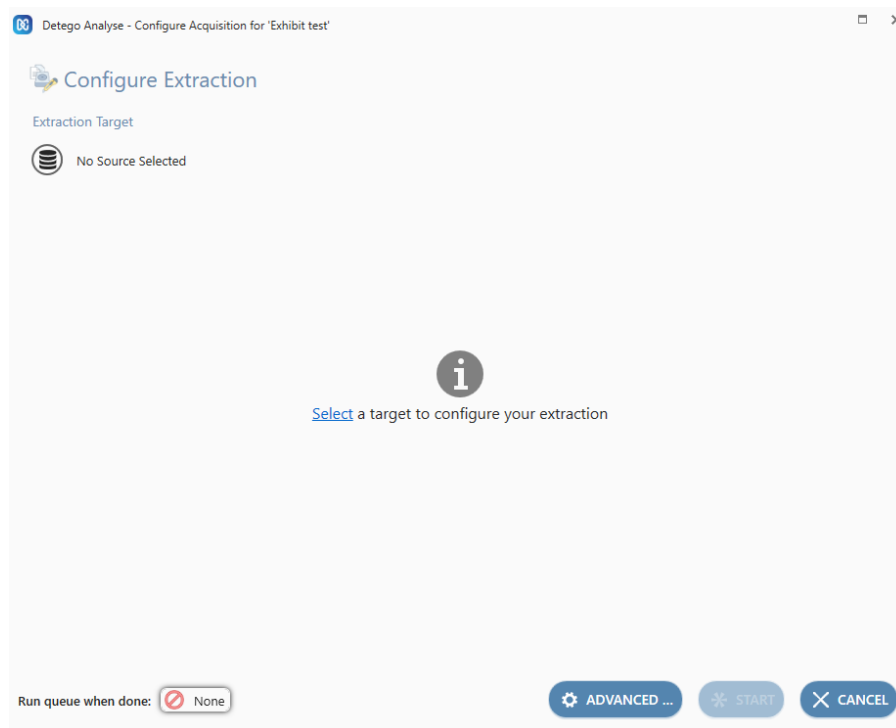
- Ensure you have created a new blank Exhibit.
- Right click on the Exhibit.
- Select the 'New Extraction' option.

Figure 353



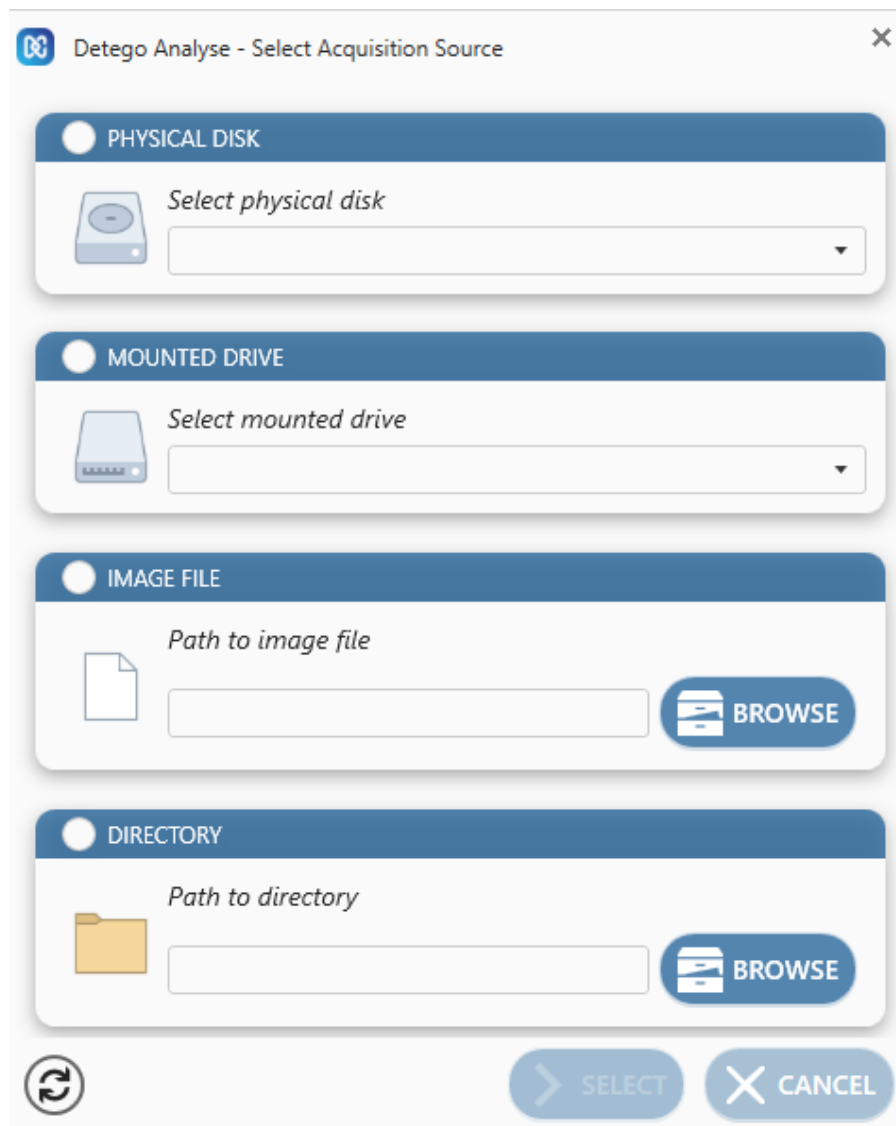
The Configure Extraction window will be displayed.

Figure 354



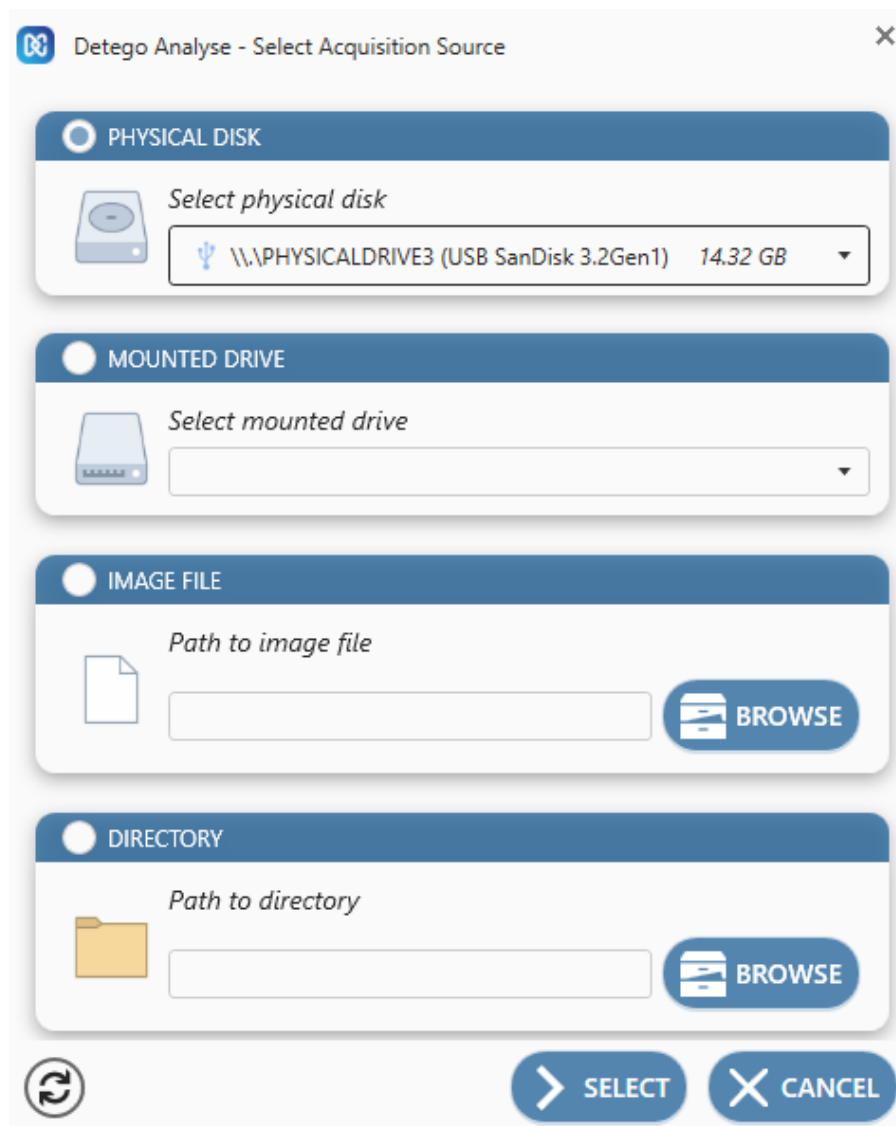
- Press 'Select' to choose your extraction target.

Figure 355



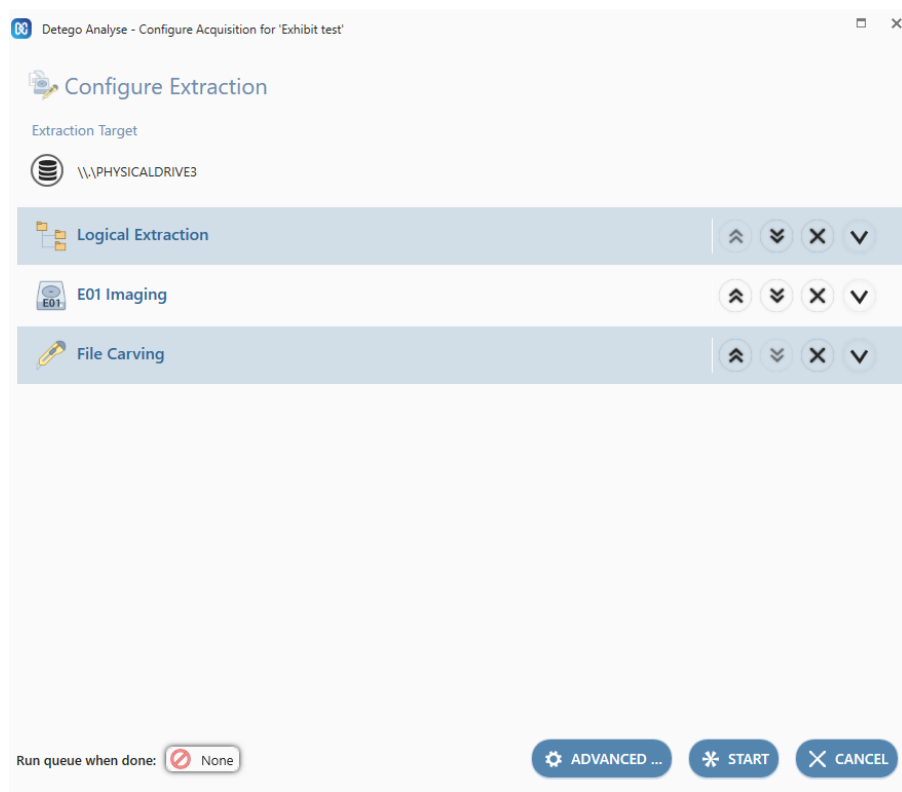
- From the options, select the type of target and the drive/file path and press the 'SELECT' button.

Figure 356



- Once selected, the default options for your target type will be applied to the Job Queue for your Extraction. E.g. A Physical Disk target will have a default job queue of:
 - Logical Extraction
 - E01 Imaging
 - File Carving

Figure 357



You can customise this extraction how you like and select 'ADVANCED' if you wish to further configure the Job Queue.

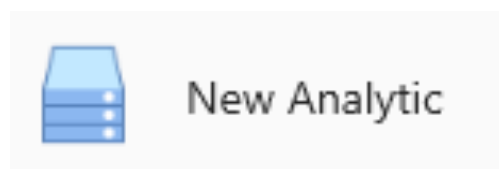
- Once you are ready, select START to initiate the Extraction.

NEW ANALYTIC

From the Case List, you can start a New Analytic. To do this, follow the below steps:

- From the Case List, right click on the Exhibit you wish to run Analytics on.
- Select the 'New Analytic' option.

Figure 358



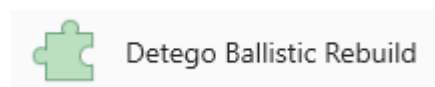
This then takes you to the Analytics screen where you can select the Analytic(s) you wish to run.

For more information, please see the Analytics section.

DETEGO BALLISTIC REBUILD

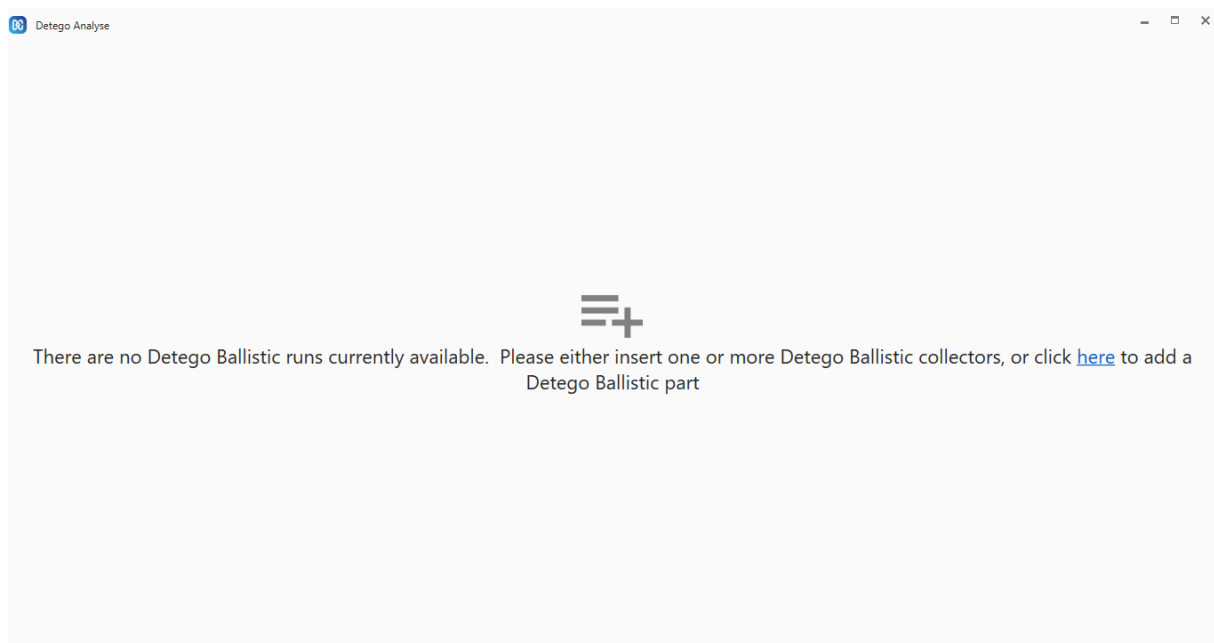
The Detego Ballistic Rebuild option allows you to manually import and rebuild a Detego Ballistic Image. This is useful when encountering issues with auto-importing of Ballistic Images or if you have the Detego Ballistic parts not on a device.

Figure 359



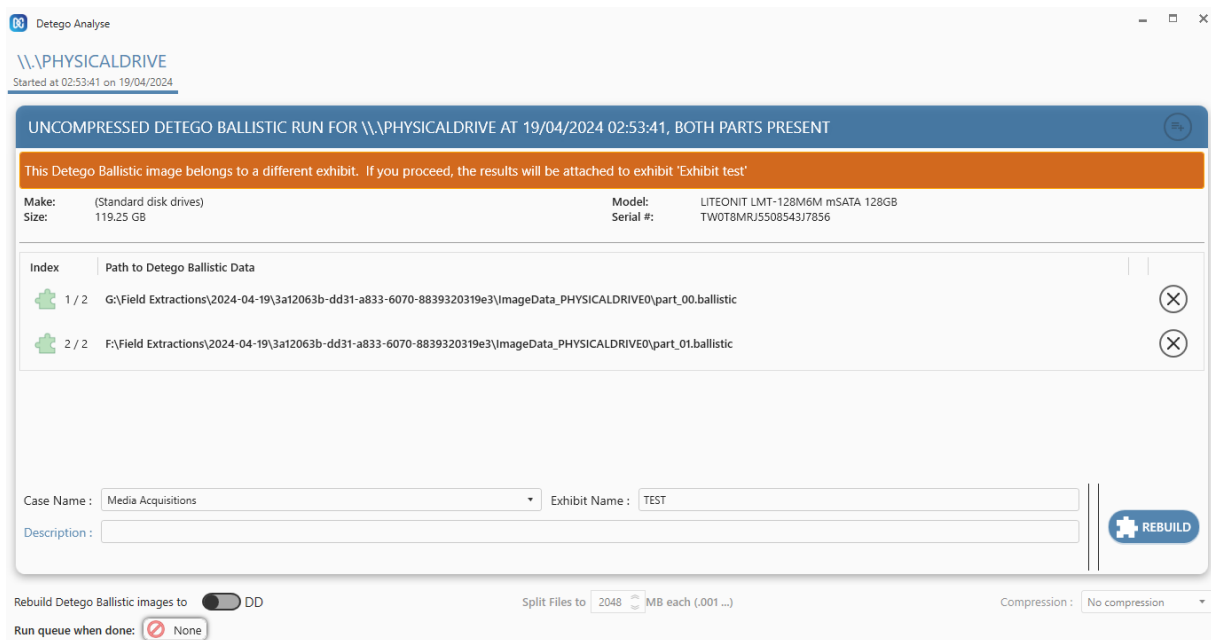
The screenshot below prompts you to insert one or more Detego Ballistic collectors or click the button 'here' to add a Detego Ballistic part. If you have a Detego Ballistic device, it will usually automatically detect if you don't have this window open; however, if it doesn't, select the 'here' button.

Figure 360



Once you select 'here', the below window will display:

Figure 361



- Select the + button to add a Detego Ballistic part.
- Select the 'Rebuild Detego Ballistic Images to' toggle button to change whether to rebuild to a DD or E01 format.
 - If toggle to E01, you can also change the split file option and the Compression option to determine if the file is split and if compression is used.
- Once you are ready, select REBUILD.

ARTEFACT_COMPARE

Artefact_Compare is a forensic comparison tool designed for scenarios where investigators need to identify changes on a device between two points in time. By comparing a clean baseline snapshot with a post-operation snapshot, the system automatically classifies every artefact as Added, Removed, Changed, or Unchanged, then creates a merged exhibit with colour-coded tags for easy analysis.

PRECONDITIONS

1. **Two exhibits required:** A pre-deployment (baseline) exhibit and a post-deployment (operational) exhibit.

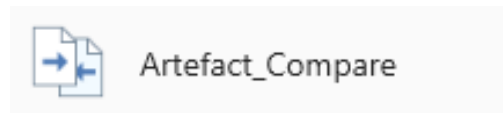
2. **Same case:** Both exhibits must belong to the same case (comparison is restricted within cases).
3. **Similar devices:** Exhibits should be from the same device at different times. However, it's possible to proceed comparison without device information in some cases.
4. **Sufficient storage:** Adequate disk space for the merged exhibit creation.

HOW TO:

To perform Artefact_Compare, follow the below steps:

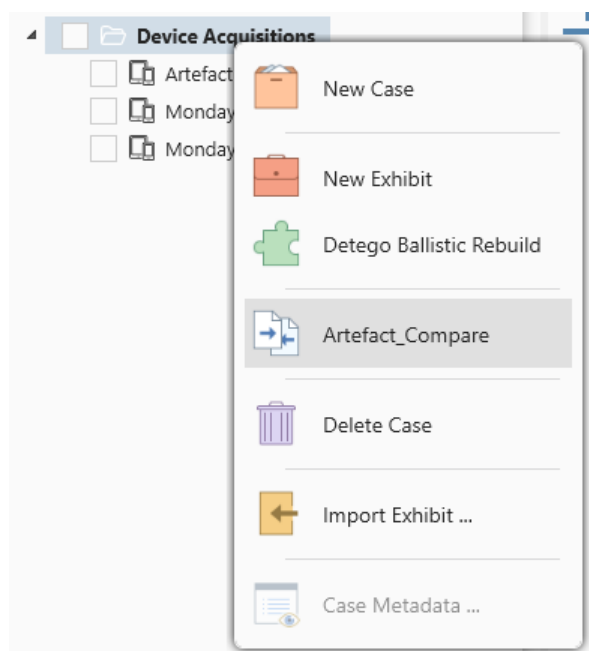
- From the Case List, right-click on either of the following:
 - The **case** containing the exhibits you want to compare
 - A specific **exhibit** within the case

Figure 362



- From the context menu, select "**Artefact_Compare**".

Figure 363



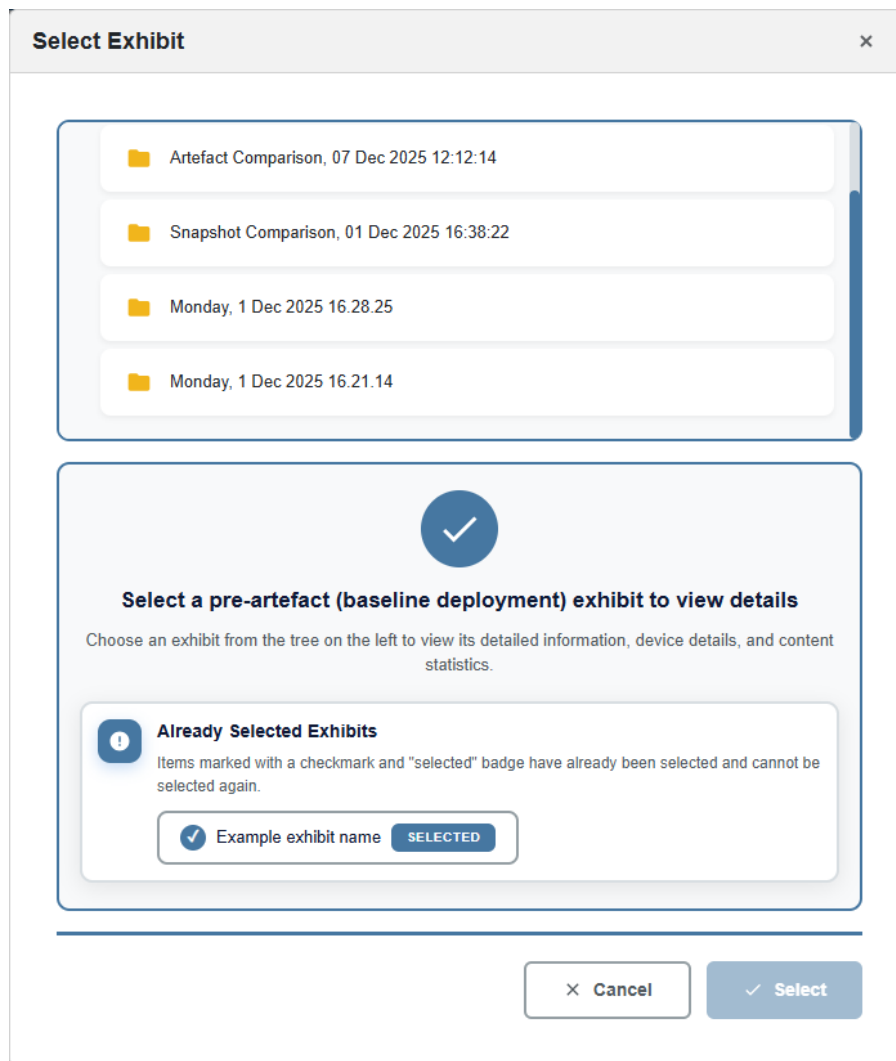
The **Artefact_Compare** interface will open:

Figure 364

The screenshot displays the 'Artefact_Compare' interface. At the top, a header bar indicates 'EXHIBIT SELECTION (0 OF 2 SELECTED)'. Below this, a 'Selection Required' message states: 'Please select both pre-deployment and post-deployment exhibits to begin comparison.' The interface is divided into two main panels: 'PRE-DEPLOYMENT (BASELINE)' and 'POST-DEPLOYMENT (AFTER OPERATION)'. Both panels show a 'NOT SELECTED' status and a 'Browse' button. Below the buttons, a dashed box contains a folder icon and the text 'No Exhibit Selected'. The 'PRE-DEPLOYMENT (BASELINE)' panel also includes the instruction 'Click "browse" to select a pre-deployment baseline exhibit'. The 'POST-DEPLOYMENT (AFTER OPERATION)' panel includes the instruction 'Click "browse" to select a post-deployment exhibit'. Below these panels, a 'COMPARISON OPTIONS' section features an 'Output Exhibit Name:' field with a placeholder 'Enter custom name...'. To the right of the field are three buttons: 'Custom', 'Auto', and 'Merge'. Below the field, a small text line reads: 'Auto: "artefact comparison - [date1] vs [date2]" • merge: "[preexhibitname] vs [postexhibitname]" • custom: enter your own'. At the bottom right, there are two buttons: 'Cancel' and 'Start Comparison'.

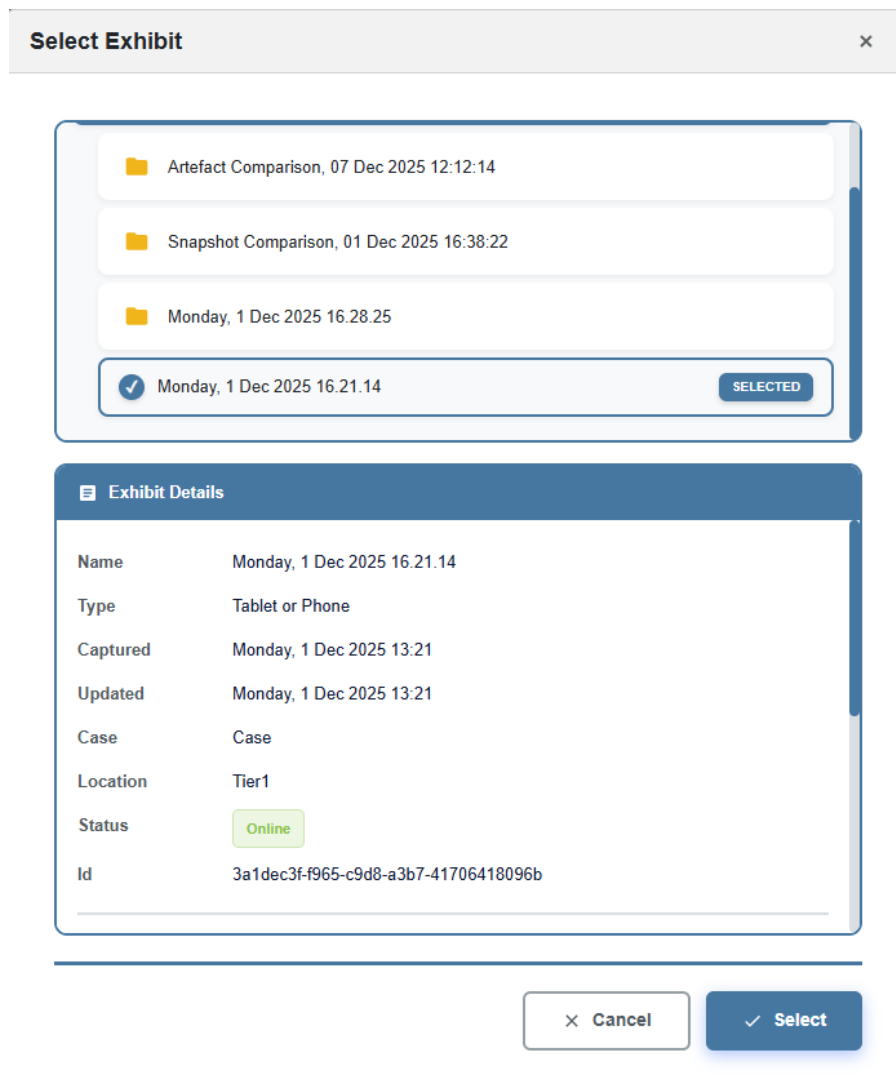
- In the **PRE-DEPLOYMENT (BASELINE)** panel on the left click the **"Browse"** button.
- The **"Select Exhibit"** dialogue opens.

Figure 365



- Select an exhibit from the list that you wish to use as your baseline (pre-deployment) exhibit.
- Once you click an exhibit, the **Exhibit Details** panel appears:

Figure 366



- After reviewing the details, click the **"Select"** button. This will return you to the **Artefact_Compare** window.
- The left panel now shows your selected pre-deployment exhibit.
- In the **POST-DEPLOYMENT (AFTER OPERATION)** panel on the right click the **"Browse"** button.
- The **"Select Exhibit"** dialogue opens again.

Figure 367

Select Exhibit

Artefact Comparison, 07 Dec 2025 12:12:14

Snapshot Comparison, 01 Dec 2025 16:38:22

Monday, 1 Dec 2025 16:28:25

SELECTED

Monday, 1 Dec 2025 16:21:14

SELECTED

Exhibit Details

Device

Mobile Device

Name:

iPhone

Model:

Apple iPhone 8

Serial #:

C8QVDM04JC67

Phone Number:

+254 740 491 275

Content Statistics

All Files (2,215)
Total Items

788.82 MB
Total Size

2,215
Live

Cancel

Select

- This time, select the exhibit captured after the device returned from field.
- After reviewing the details, click the **"Select"** button. This will return you to the **Artefact_Compare** window.

After selecting both exhibits, the Artefact_Compare window updates:

Figure 368

EXHIBIT SELECTION (2 OF 2 SELECTED)

PRE-DEPLOYMENT (BASELINE)

Monday, 1 Dec 2025 16.21.14

Exhibit Information

Exhibit Name: Monday, 1 Dec 2025 16.21.14

Exhibit Id: 3a1dec3f4965-c9d8-a3b7-41706418096b

File types (scroll for more):

- Archive: 14 files (255.44 MB)
- Code: 9 files (772.39 KB)
- Cryptography: 2 files (1.84 KB)

POST-DEPLOYMENT (AFTER OPERATION)

Monday, 1 Dec 2025 16.28.25

Exhibit Information

Exhibit Name: Monday, 1 Dec 2025 16.28.25

Exhibit Id: 3a1dec46-8fc7-73c6-4c57-202e4f532d1a

File types (scroll for more):

- Archive: 14 files (255.44 MB)
- Code: 9 files (772.39 KB)
- Cryptography: 2 files (1.84 KB)

Quick Summary

Device Match: ☒ Same device (serial numbers match)

Date Sequence: ☒ Valid (pre before post)

Item Difference: -129 items (2,215 - 2,344)

Size Difference: -60.53 MB (788.82 MB - 849.35 MB)

COMPARISON OPTIONS

Output Exhibit Name:

Artefact Comparison, 08 Dec 2025 10:38:03

Auto: "artefact comparison - [date1] vs [date2]" • merge: "[preexhibitname] vs [postexhibitname]" • custom: enter your own

Custom Auto Merge

✓ Ready to Compare: All validation checks passed

Cancel Start Comparison

- Verify both exhibits are correct.
- Review the Quick Summary validation checks.
- Ensure all checks show checkmarks.
- Optionally customize the output exhibit name.
- Click the **"Start Comparison"** button.

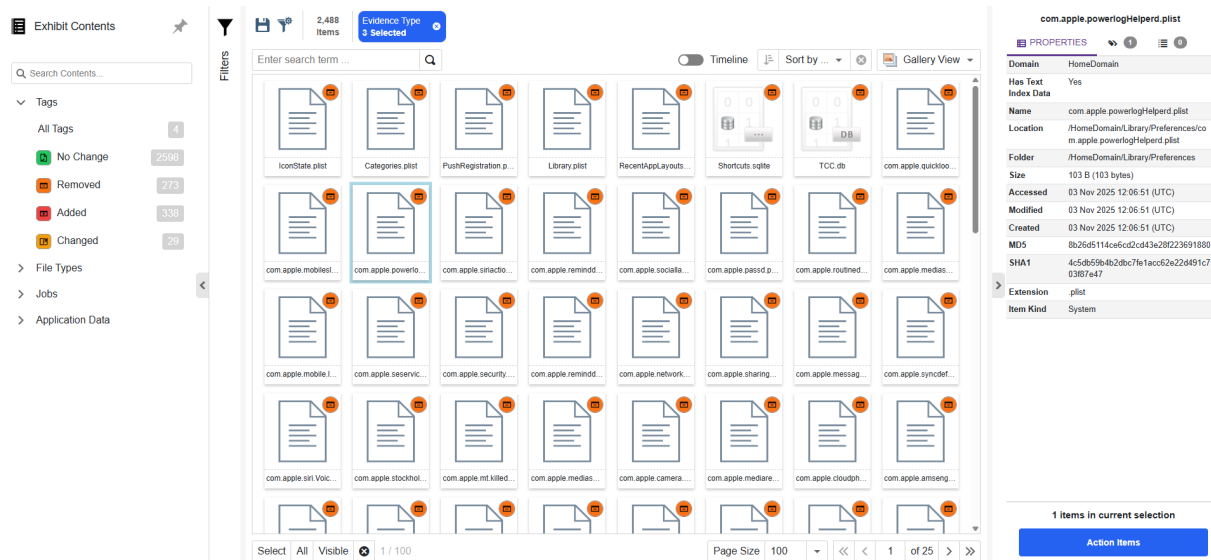
When the comparison job completes:

- **Job Progress** shows 100% completion.
- A new **merged exhibit** appears in your Case List.
- The merged exhibit name is what you configured (or auto-generated).

- Navigate to the merged exhibit in the Case List.
- Open the **Evidence Browser** for the merged exhibit.

The Evidence Browser shows all items from both exhibits:

Figure 369



Tags Panel (Left Side)

The **Tags** section shows the comparison classification tags:

All Tags: 4

1. ● No Change

- Items identical in both exhibits.
- Usually filtered out to focus on changes.

2. ● Removed

- Items present in baseline but missing in post-deployment.
- Deleted or removed during operation.

3. ● Added

- Items not in baseline but present in post-deployment.

- b. New files created during operation.

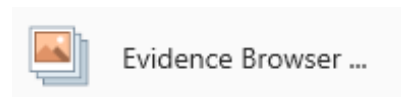
4. Changed

- a. Items present in both but with different properties.
- b. Modified content, moved location, or updated metadata.

EVIDENCE BROWSER

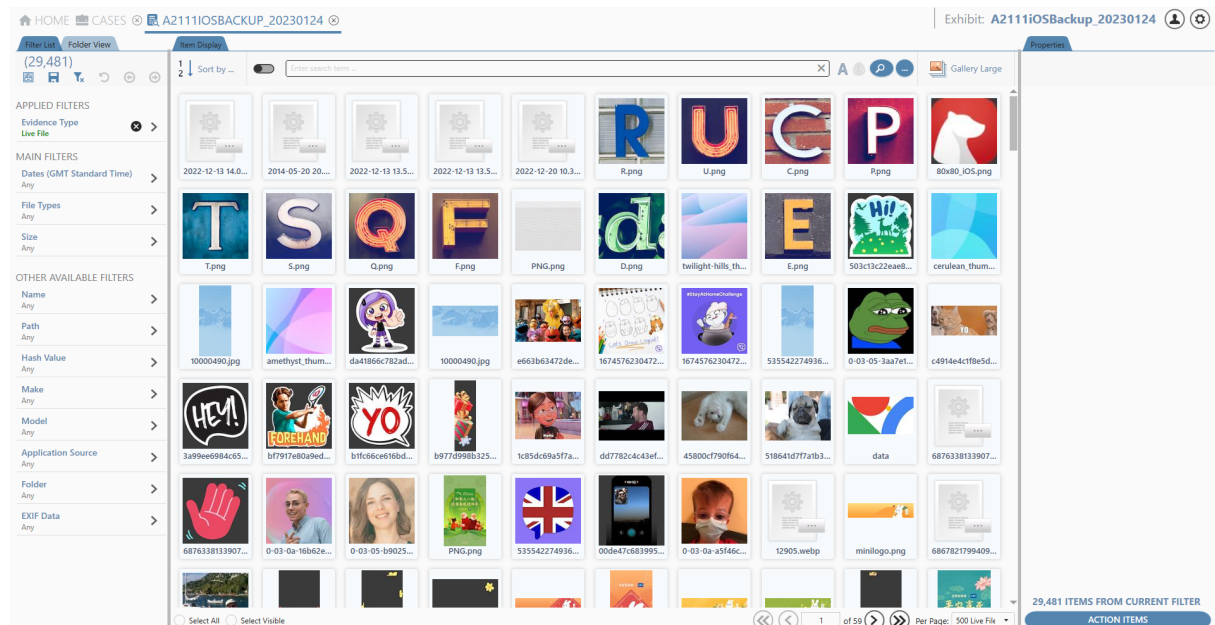
The Evidence Browser option will take you straight to the Evidence Browser of the exhibit.

Figure 370



This will open All Live Files by default.

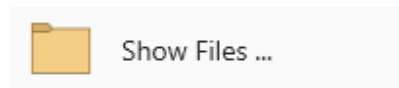
Figure 371



SHOW FILES

The 'Show Files ...' option allows you to view the raw database filesystem of where the exhibit files are stored.

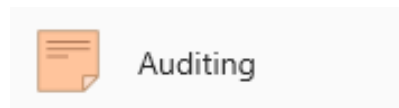
Figure 372



AUDITING

Selecting the 'Auditing' option will take you straight to the Audit Log screen within your exhibit.

Figure 373

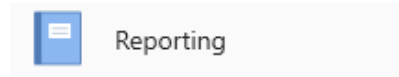


For more information, go to the Audit Log section.

REPORTING

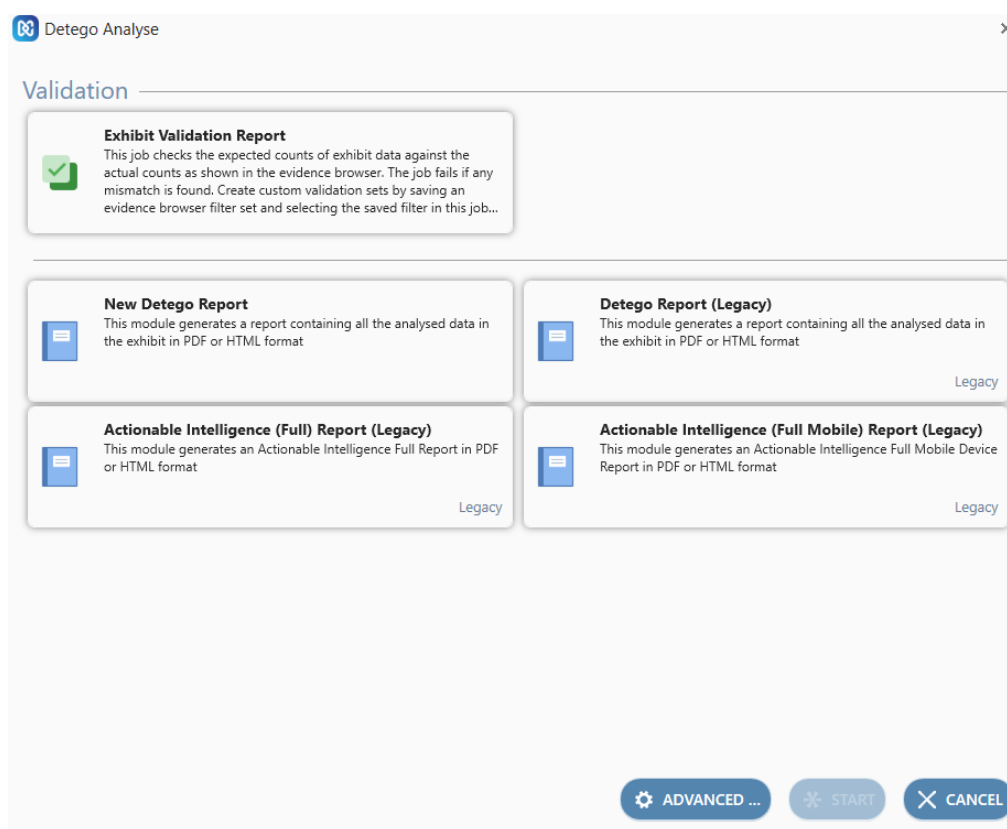
The Reporting button takes you straight to the Report action.

Figure 374



This will open the Report window where you can select which report you would like to run.

Figure 375

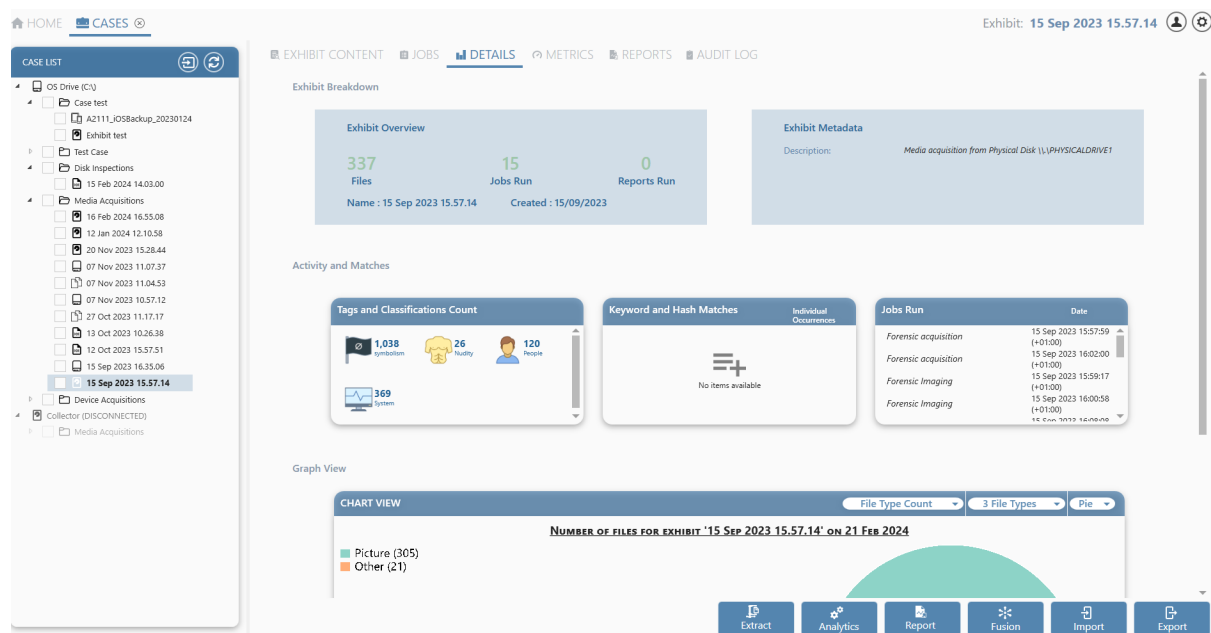


For more information, go to the Reports section.

DETAILS TAB

The Details tab will display the basic details of the currently selected drive, case or exhibit.

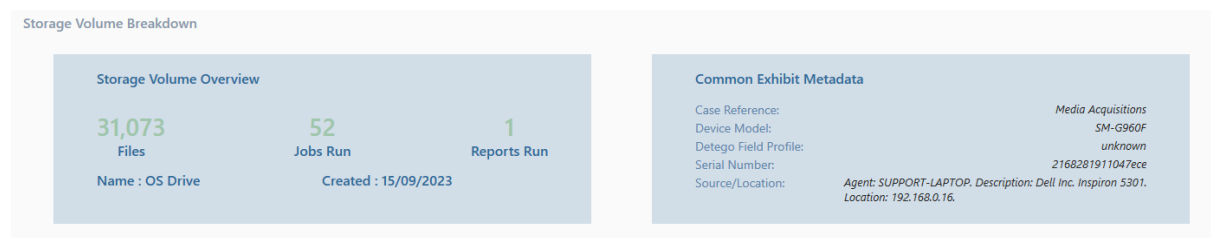
Figure 376



STORAGE VOLUME BREAKDOWN

If you have a storage volume selected in your Case List, you will see the Storage Volume Breakdown section under the DETAILS tab.

Figure 377

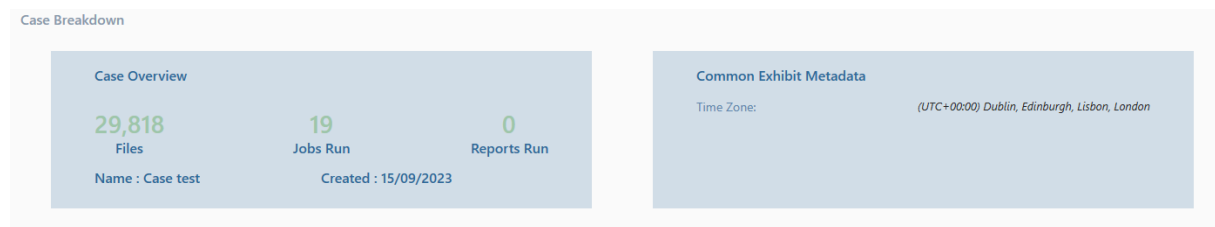


- **Storage Volume Overview** - This displays a brief outline of the number of files in the cases/exhibits, the number of jobs and reports run as well as the name and the date the storage volume was created.
- **Common Exhibit Metadata** - This displays the common exhibit metadata which varies depending on your exhibits.

CASE BREAKDOWN

If you have a Case selected in your Case List, you will see the Case Breakdown section under the DETAILS tab.

Figure 378

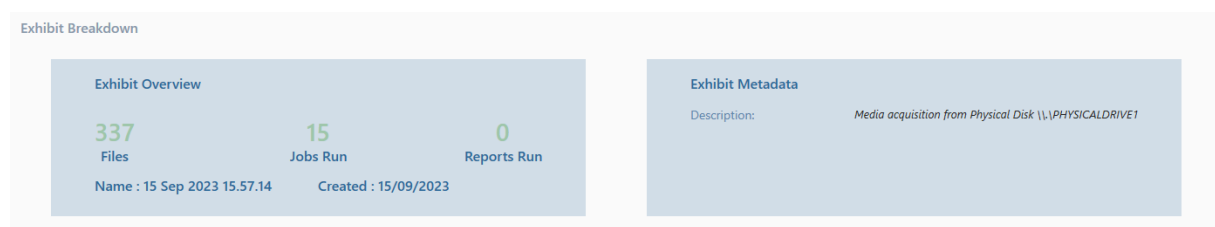


- **Case Overview** - This displays a brief outline of the number of files in the case, the number of jobs and reports run as well as the name and the date the case was created.
- **Common Exhibit Metadata** - This displays the common exhibit metadata which varies depending on your exhibits.

EXHIBIT BREAKDOWN

If you have an exhibit selected, you will see the Exhibit Breakdown

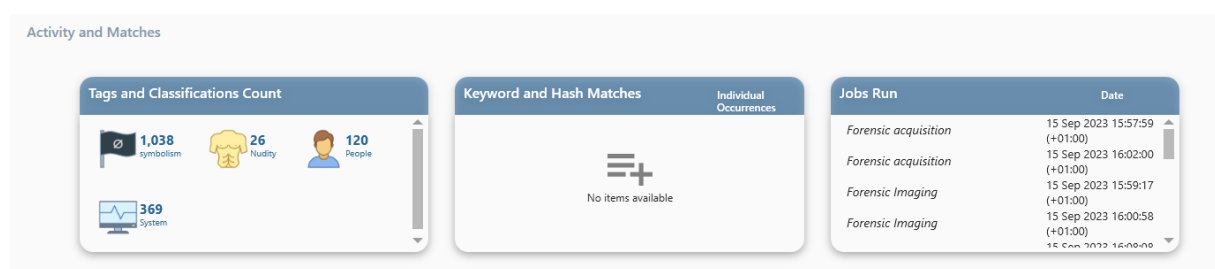
Figure 379



- **Exhibit Overview** - This displays a brief outline of the number of files in the exhibits, the number of jobs and reports run as well as the name and the date the exhibit was created.
- **Exhibit Metadata** - This displays the exhibit metadata which varies depending on your exhibit.

ACTIVITY AND MATCHES

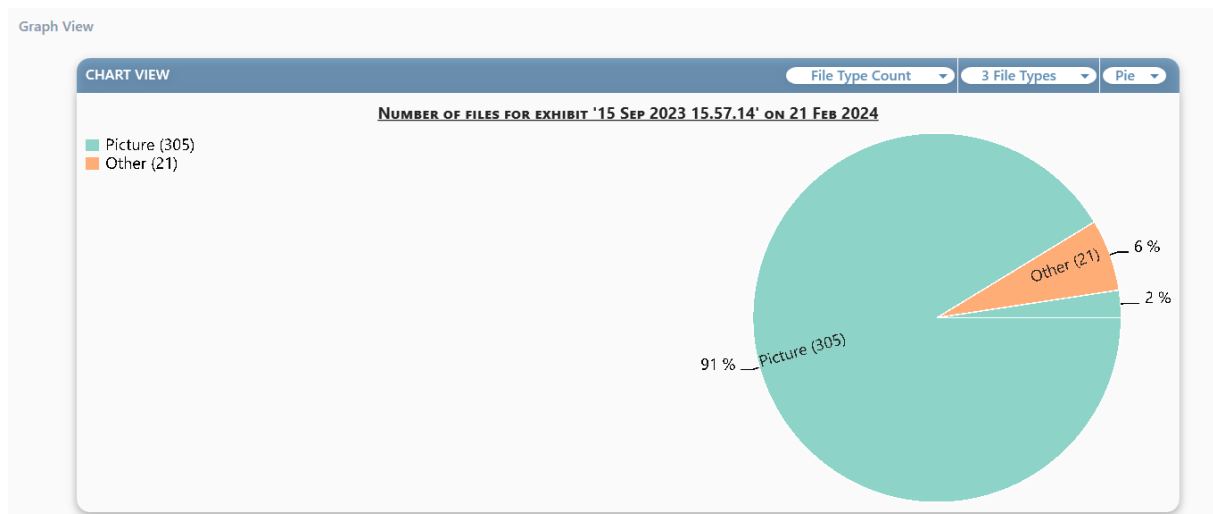
Figure 380



- **Tags and Classifications Count** - This displays the number of tags and classifications in the cases/exhibits.
- **Keyword and Hash Matches** - This displays the keyword and hash matches that have been run and the number of hits for each list.
- **Jobs Run** - This displays the different jobs that have been run and the timestamp of when they were run.

GRAPH VIEW

Figure 381



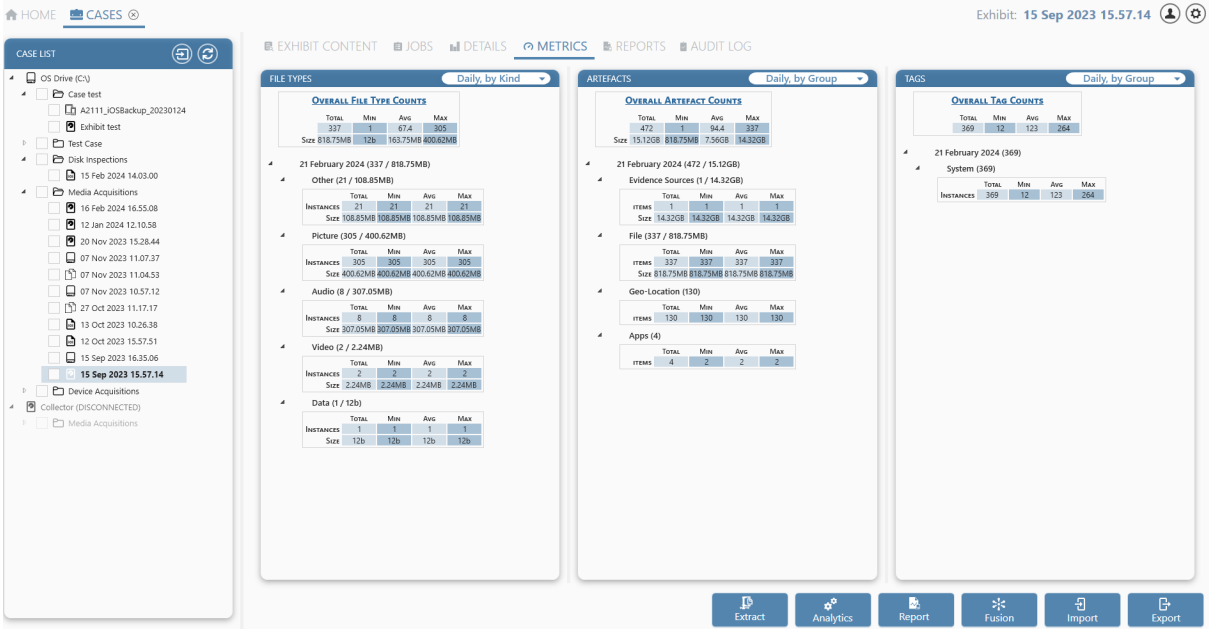
- **Chart View** - This displays a chart of various information which can give you an idea of how much an exhibit(s) consists of picture files against other files, etc. You can use the dropdowns to customise how this is displayed and what information it shows.

METRICS TAB

The METRICS tab shows all the metrics for the case or exhibit you have selected, including File Types, Artefacts and Tags.

- You can select the small arrow next to each dropdown to expand or collapse each dropdown, displaying the different metrics.
- You also have the ability to change how they are displayed using the dropdowns at the top of each section.

Figure 382



6.2. IMPORTING EXHIBITS

You can import multiple types of exhibits into Detego.

These include the below:

PHYSICAL IMAGE IMPORTER

This moves or copies an existing physical image into a case/exhibit, then is tracked and audited by the case management system. Once imported, Detego can perform extractions and analysis jobs on the image.

Figure 383

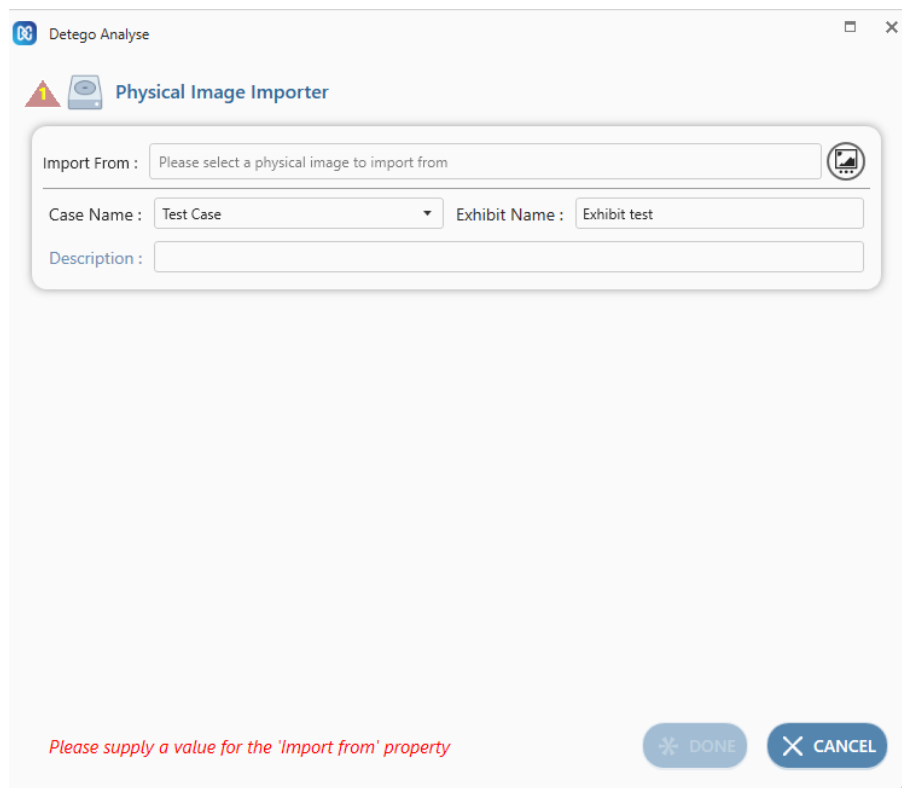


Physical Image Importer

Moves or makes a copy of an existing physical image into a case/exhibit which is then tracked and audited by the case management system. Once imported Detego can then perform extractions and analysis jobs on the...

Once you have selected the tile, the Physical Image Importer screen will open.

Figure 384



- 'Import From' - Browse for the Image file you wish to import.
- 'Case Name:' - Name of the Case you wish to import it into.
- 'Exhibit Name:' - Name of the Exhibit you wish to call it.
- 'Description:' - Any description of the Exhibit you wish to include if any.

MSAB IMPORTER

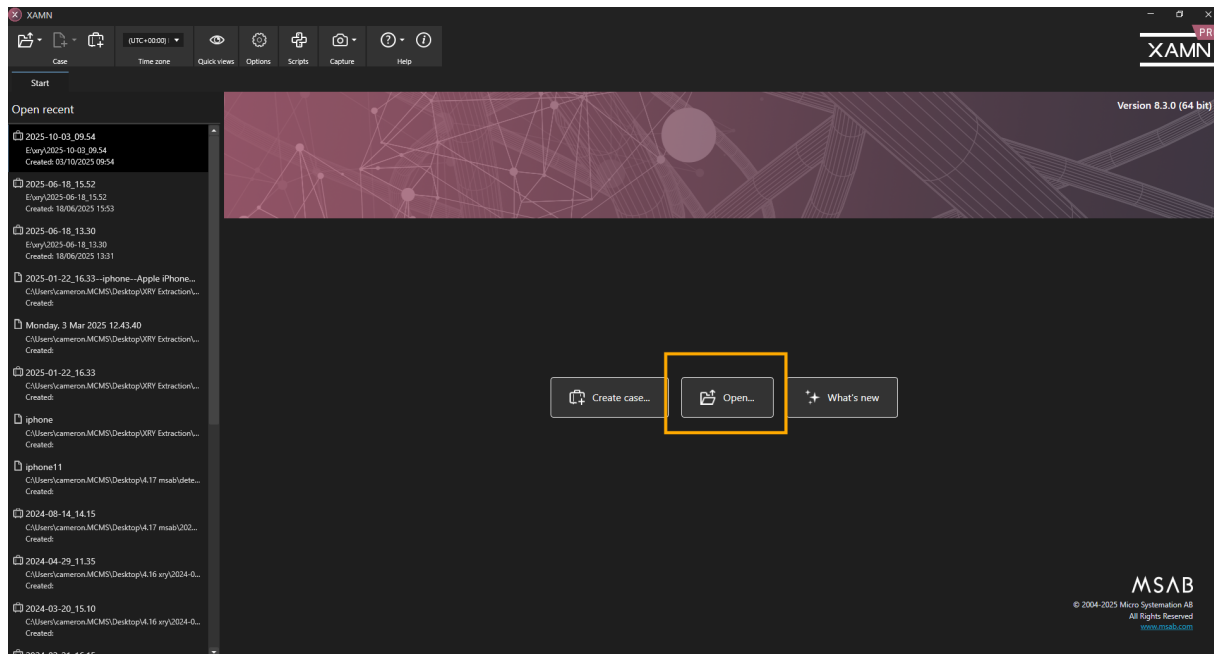
This turns an MSAB export file (.msabnuix) into a Detego case.

Detego Analyse can import .msabdetego files. The ability to export an XRY file into a .msabdetego file is in XAMN version 7.050.2495 or later.

An active license for Detego Analyse and MSAB XAMN will be required before proceeding.

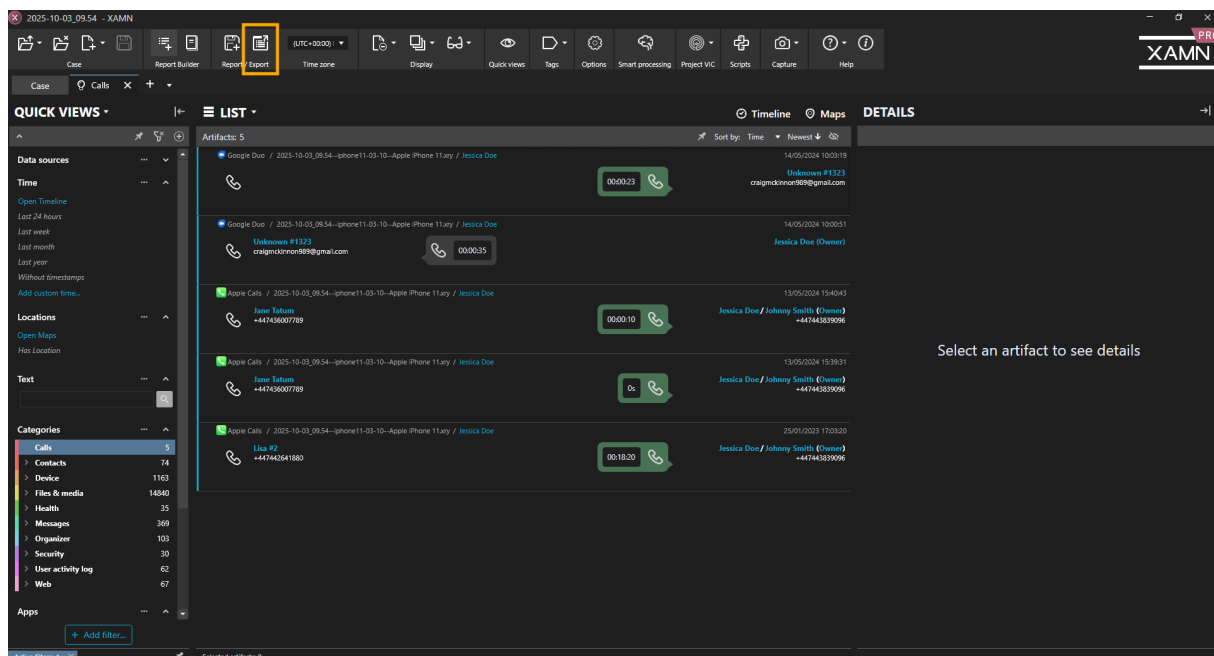
- Open MSAB XAMN and select the 'Open' tile

Figure 385



- Select the .xry file you wish to import
- Once imported select the 'Export' button at the top

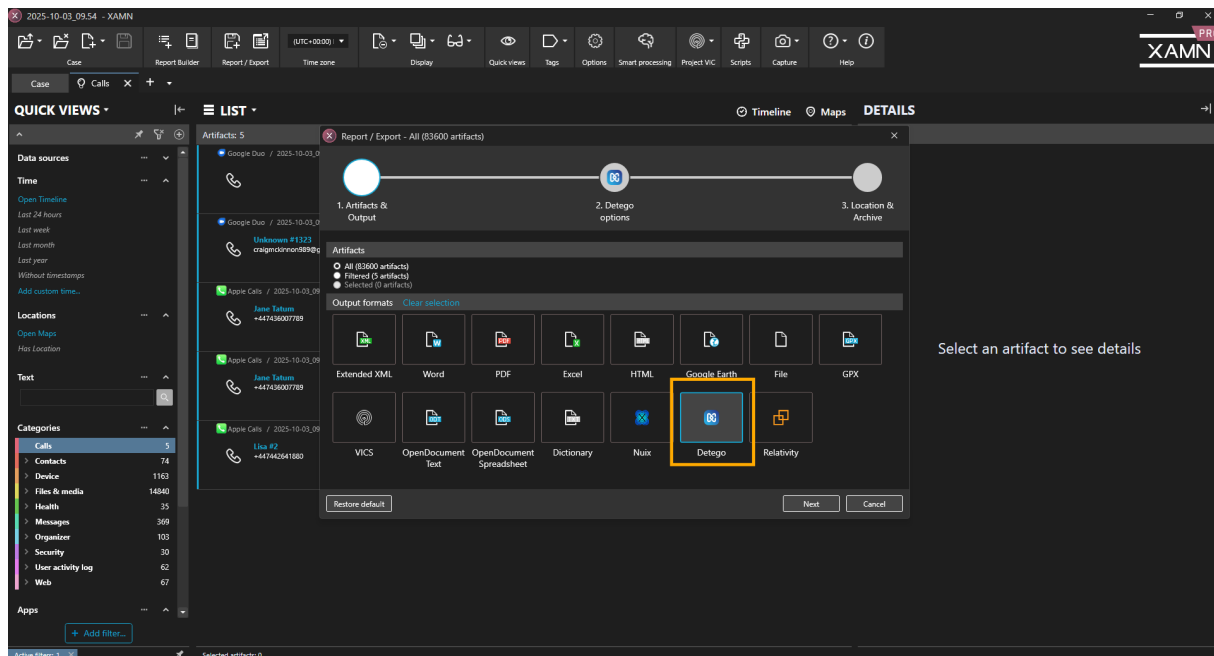
Figure 386



- Select the Artifacts you wish to include
 - You can choose to include all

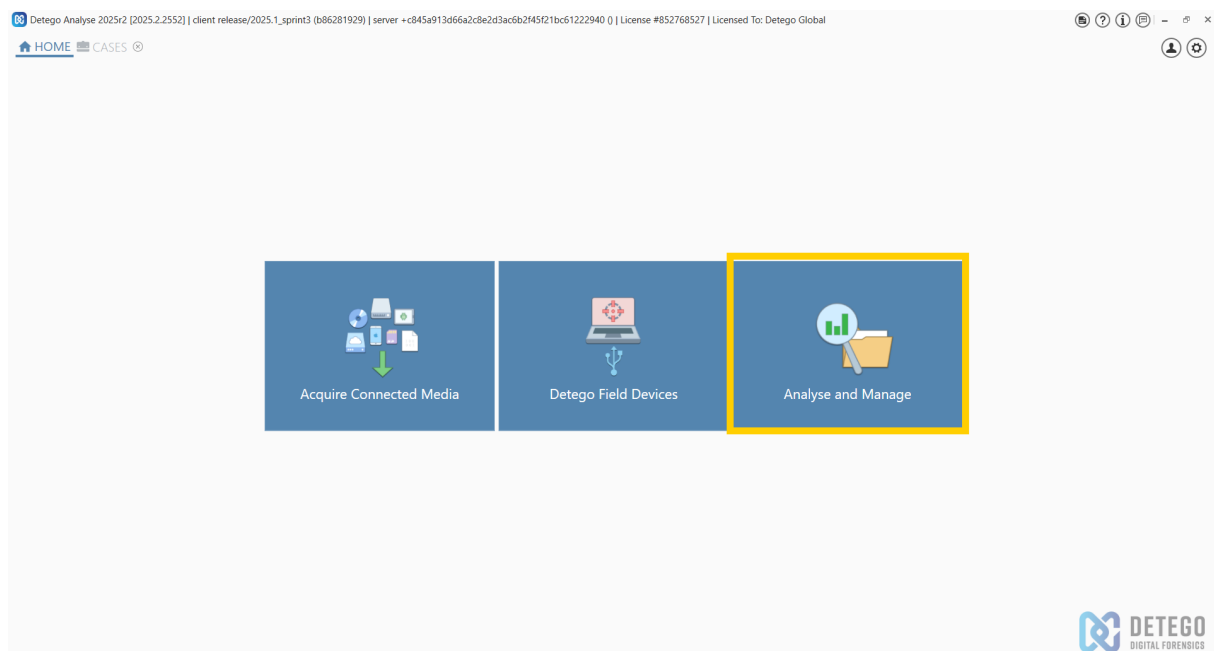
- Makes sure to select the 'Detego' option

Figure 387



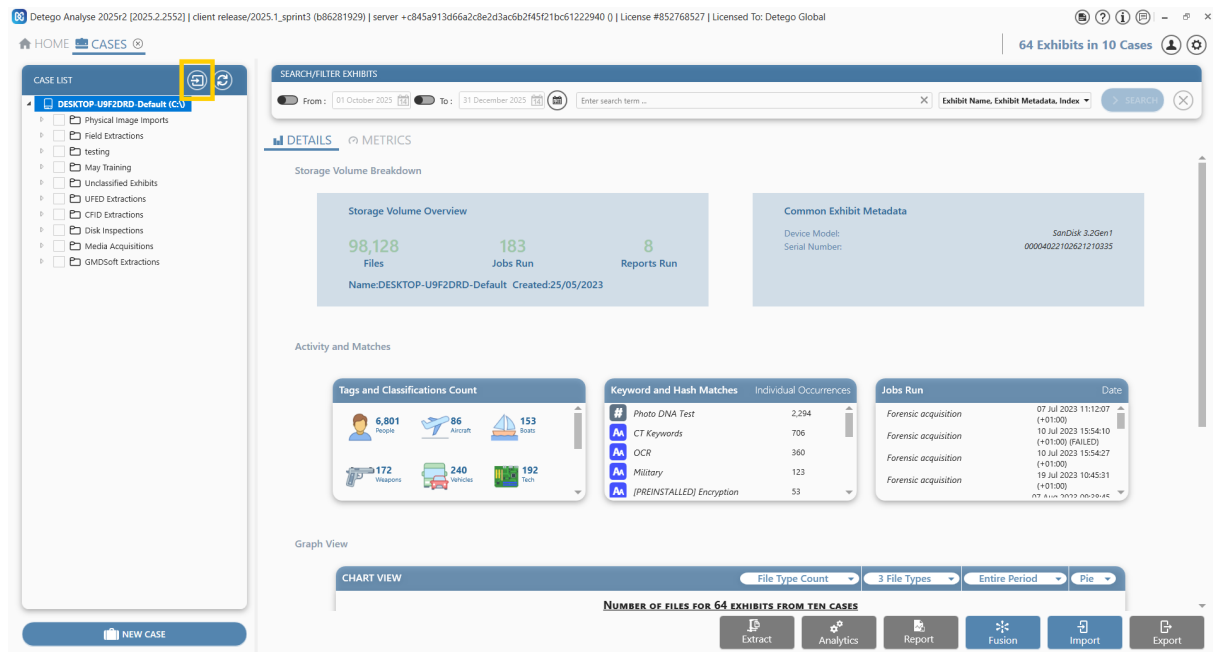
- Once exported open up Detego Analyse and Select the Analyse and Manage tile

Figure 388



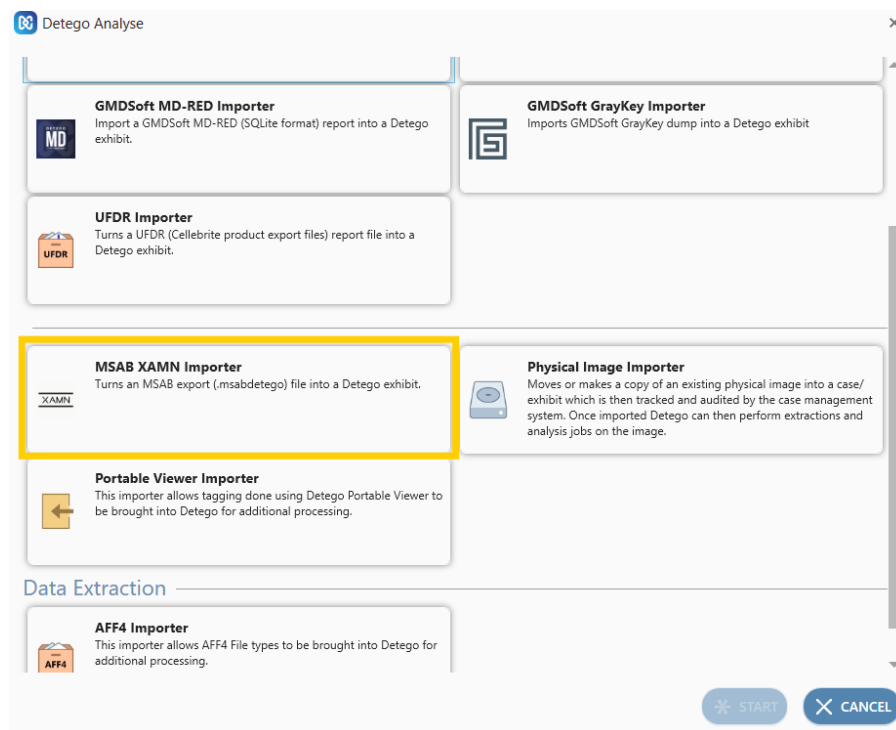
- Select the 'Import' button on the 'Case List'

Figure 389



- Choose the 'MSAB XAMN Importer'

Figure 390



- Select the .msabdeteo file you exported from MSAB XAMN
- Click 'Done'

- Click 'Start'

PORTABLE VIEWER IMPORTER

This allows tagging done using Detego Portable Viewer to be brought into Detego® Analyse for additional processing.

Figure 391

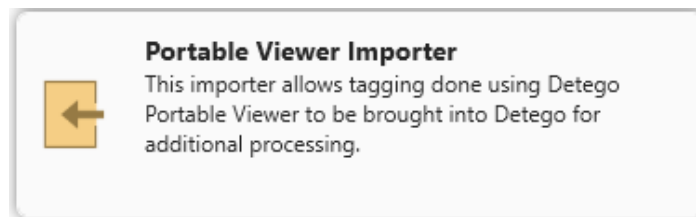
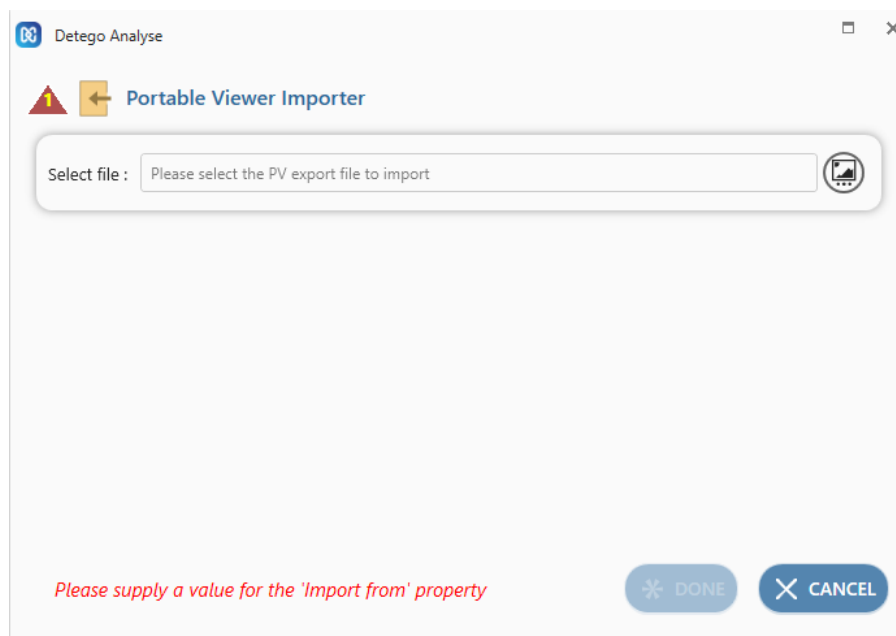


Figure 392



DETEGO PACKAGE IMPORT

This imports an entire exhibit, including all binary artefacts and database entries, from an archive transferred from another system.

Figure 393

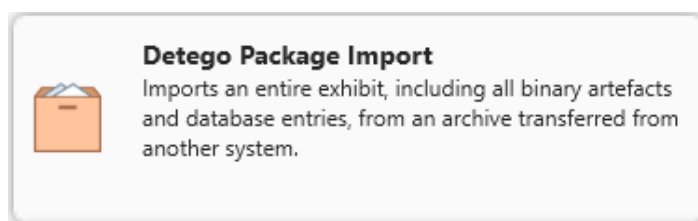
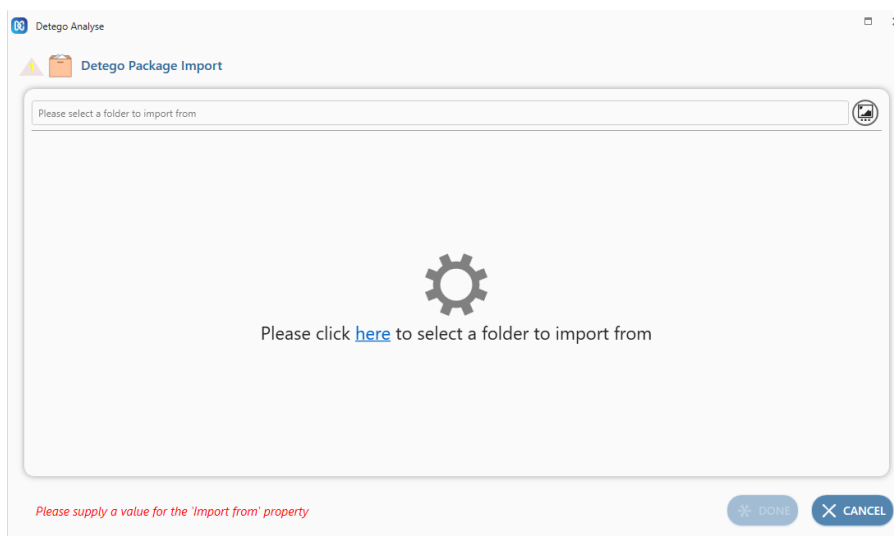


Figure 394



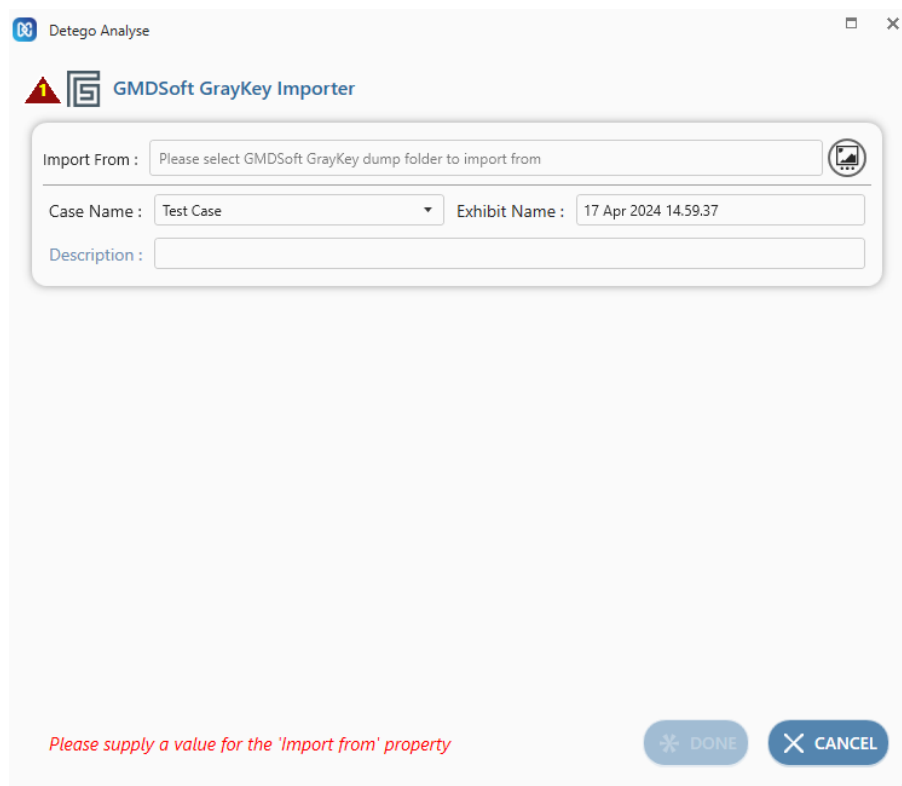
GMDSOFT GRAYKEY IMPORTER

Will import a GrayKey extraction from GMDSOFT into a Detego Exhibit.

Figure 395



Figure 396



Detego Analyse

GMDSoft GrayKey Importer

Import From : Please select GMDSoft GrayKey dump folder to import from

Case Name : Test Case Exhibit Name : 17 Apr 2024 14:59:37

Description :

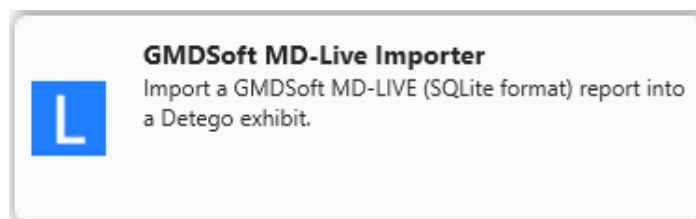
Please supply a value for the 'Import from' property

DONE CANCEL

GMDSOFT MD-LIVE IMPORTER

Will import a GMDSOFT MD-LIVE (SQLite format) report into a Detego exhibit.

Figure 397



GMDSoft MD-Live Importer

Import a GMDSoft MD-LIVE (SQLite format) report into a Detego exhibit.

Figure 398

Detego Analyse

GMDSoft MD-Live Importer

Import From : Please select GMDSoft MD-Live (SQLite format) Report folder to import from

Case Name : Test Case Exhibit Name : 17 Apr 2024 15.04.21

Description :

Please supply a value for the 'Import from' property

DONE CANCEL

UFDR IMPORTER

This turns a UFDR (Cellebrite product export files) report into a Detego exhibit.

Figure 399

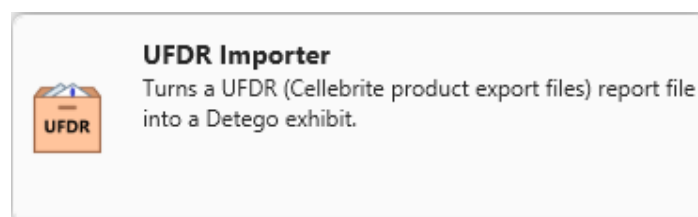
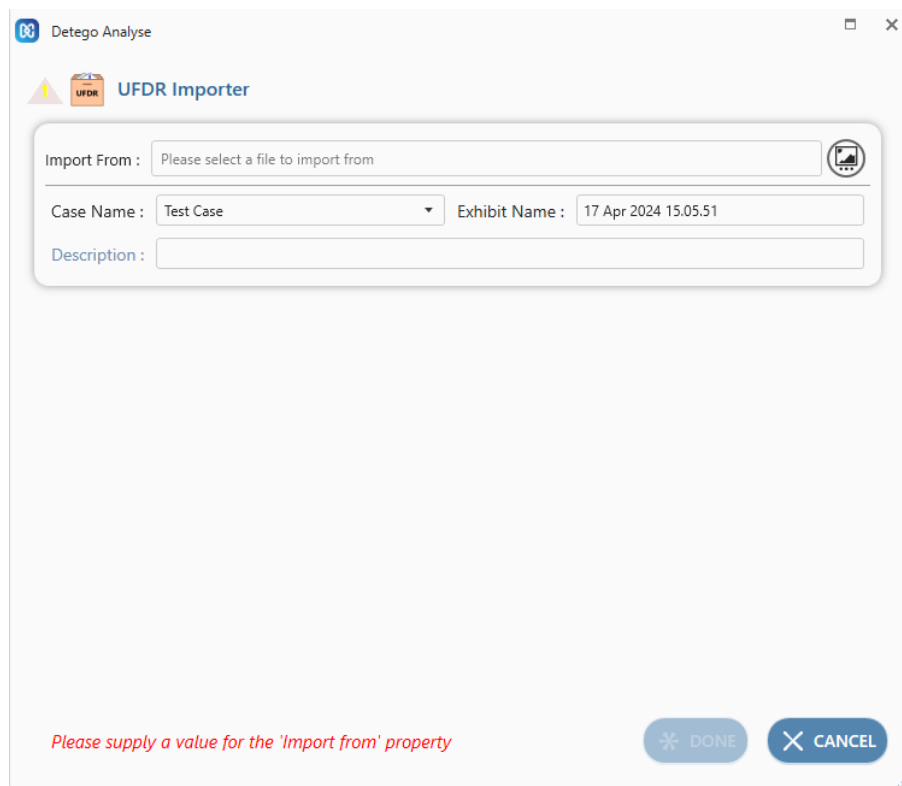


Figure 400



The screenshot shows a window titled "Detego Analyse" with a sub-header "UFD Importer". Inside the window, there is a form with the following fields:

- Import From :** A text input field with the placeholder text "Please select a file to import from" and a file selection icon on the right.
- Case Name :** A dropdown menu currently showing "Test Case".
- Exhibit Name :** A text input field containing "17 Apr 2024 15.05.51".
- Description :** An empty text input field.

At the bottom of the window, there is a red error message: "Please supply a value for the 'Import from' property". To the right of the message are two buttons: "DONE" (disabled, indicated by a greyed-out asterisk icon) and "CANCEL".

CFID IMPORTER

This allows data acquired from the CFID device to be brought into Detego Analyse for additional processing.

When extracting Drone flights please use the 'All Flights - Logical' option to allow the data to be imported into Detego Analyse.

Figure 401

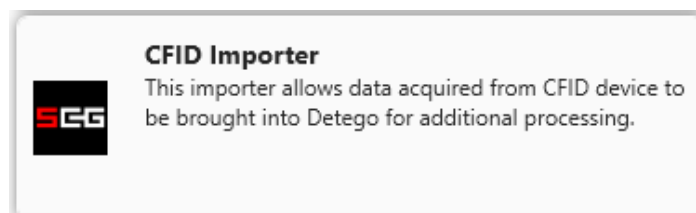
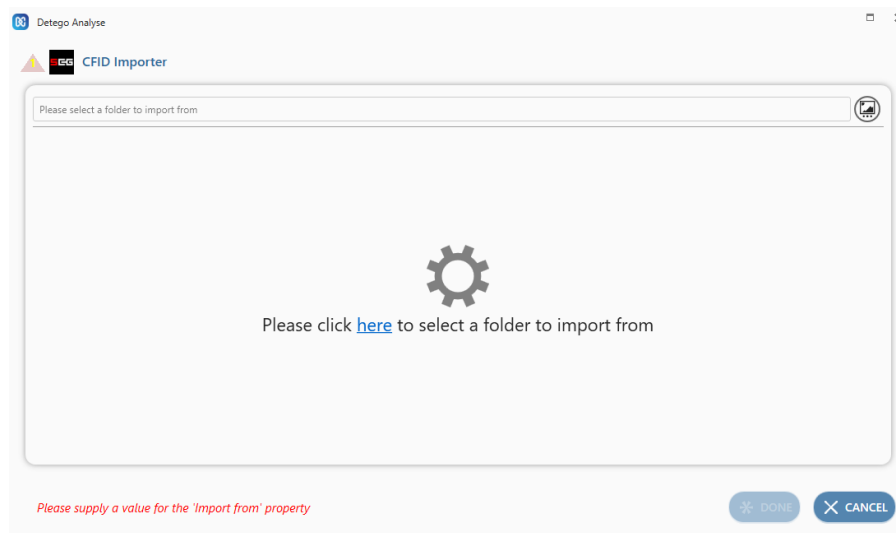


Figure 402



GMDSOFT MD-RED IMPORTER

Will import a GMDSOFT MD-RED (SQLite format) report into a Detego exhibit.

Figure 403

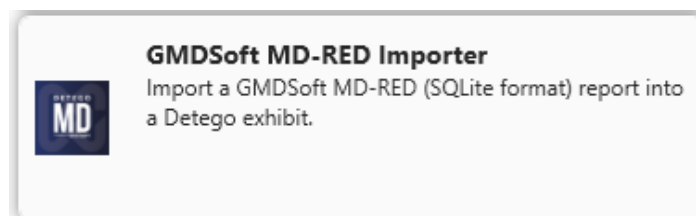
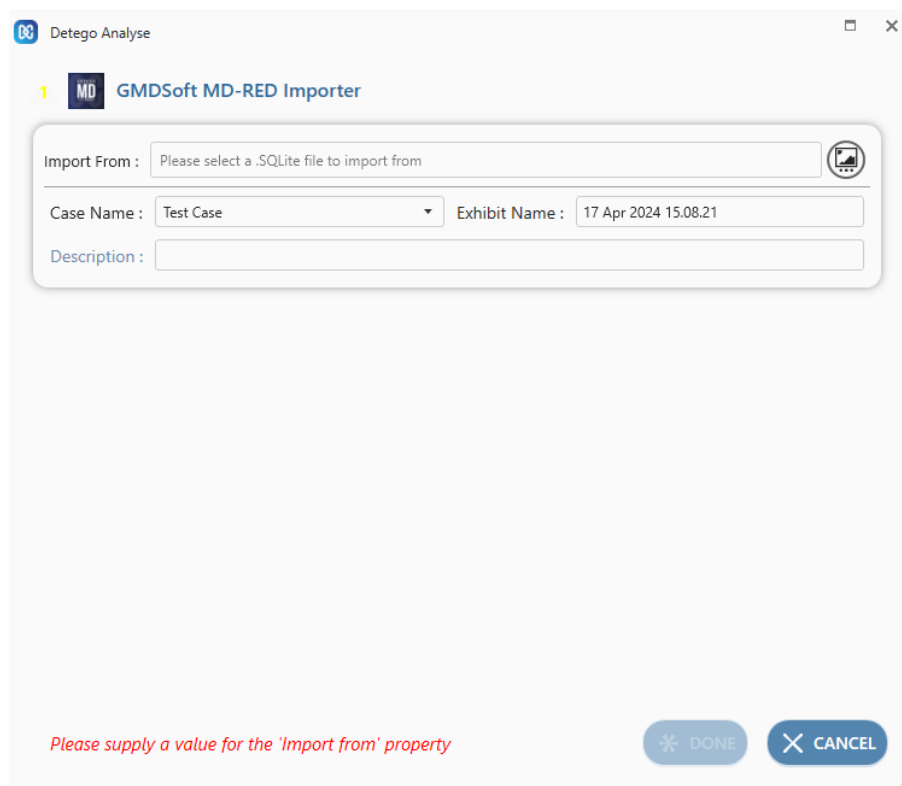


Figure 404



The screenshot shows a window titled "Detego Analyse" with a sub-header "1 MD GMDSoft MD-RED Importer". The main area contains a form with the following fields:

- Import From :** A text input field with the placeholder "Please select a .SQLite file to import from" and a file selection icon on the right.
- Case Name :** A dropdown menu currently showing "Test Case".
- Exhibit Name :** A text input field containing "17 Apr 2024 15.08.21".
- Description :** An empty text input field.

At the bottom left, there is a red error message: "Please supply a value for the 'Import from' property". At the bottom right, there are two buttons: "DONE" (with a checkmark icon) and "CANCEL" (with an 'X' icon).

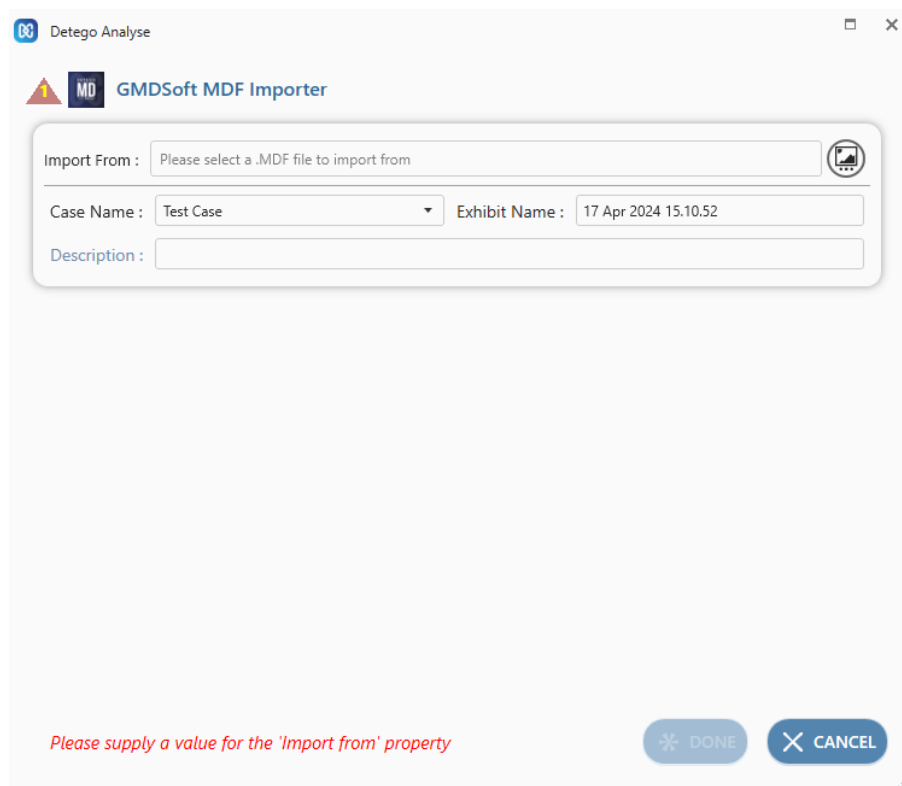
GMDSOFT MDF IMPORTER

Imports a GMDSOFT extraction into a Detego exhibit.

Figure 405



Figure 406



The screenshot shows a window titled "Detego Analyse" with a sub-header "GMDSoft MDF Importer". Inside the window, there is a form with the following fields:

- Import From :** A text input field with the placeholder text "Please select a .MDF file to import from" and a file selection icon on the right.
- Case Name :** A dropdown menu currently showing "Test Case".
- Exhibit Name :** A text input field containing "17 Apr 2024 15.10.52".
- Description :** An empty text input field.

At the bottom of the window, there is a red error message: "Please supply a value for the 'Import from' property". To the right of the message are two buttons: "DONE" and "CANCEL".

AFF4 IMPORTER

We added the ability to import AFF4 files into Detego Analyse for further processing. The exhibit is created under **Physical Image Imports**.

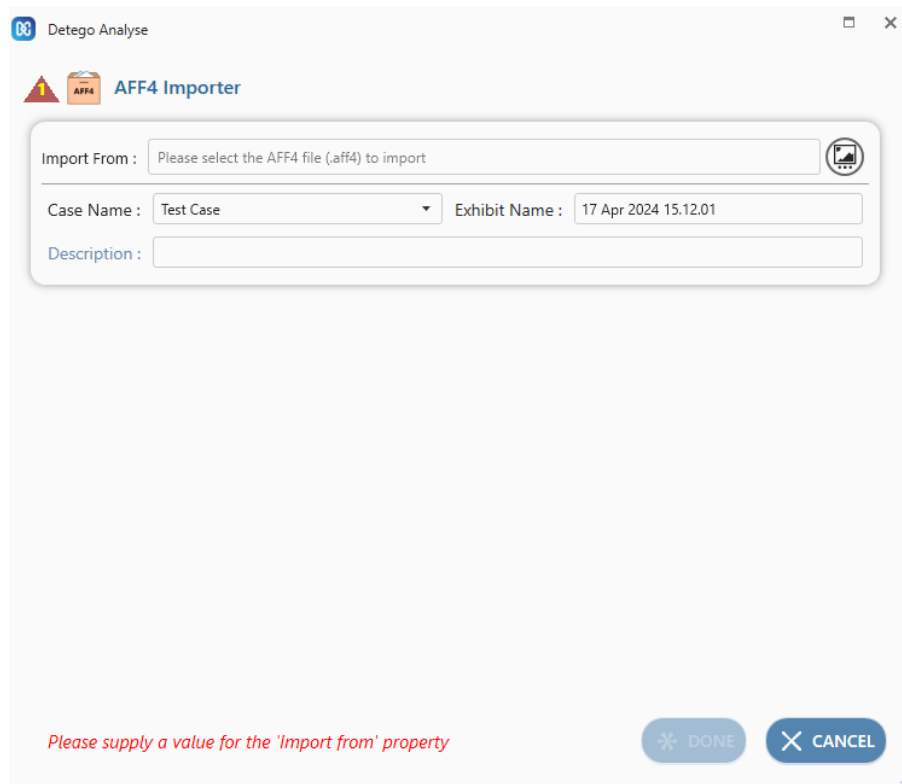
- To import an AFF4, click import in the cases list and select AFF4 Importer.

Figure 407



- Select the AFF4 file to import, click done, and start the import job. The Exhibit details will be populated from the AFF4 details and can be edited.

Figure 408



The screenshot shows a window titled "Detego Analyse" with a sub-dialog titled "AFF4 Importer". The dialog contains the following fields:

- Import From :** A text input field with the placeholder text "Please select the AFF4 file (.aff4) to import" and a file selection icon on the right.
- Case Name :** A dropdown menu currently showing "Test Case".
- Exhibit Name :** A text input field containing "17 Apr 2024 15.12.01".
- Description :** An empty text input field.

At the bottom of the dialog, there is a red error message: "Please supply a value for the 'Import from' property". To the right of the message are two buttons: "DONE" (disabled) and "CANCEL".

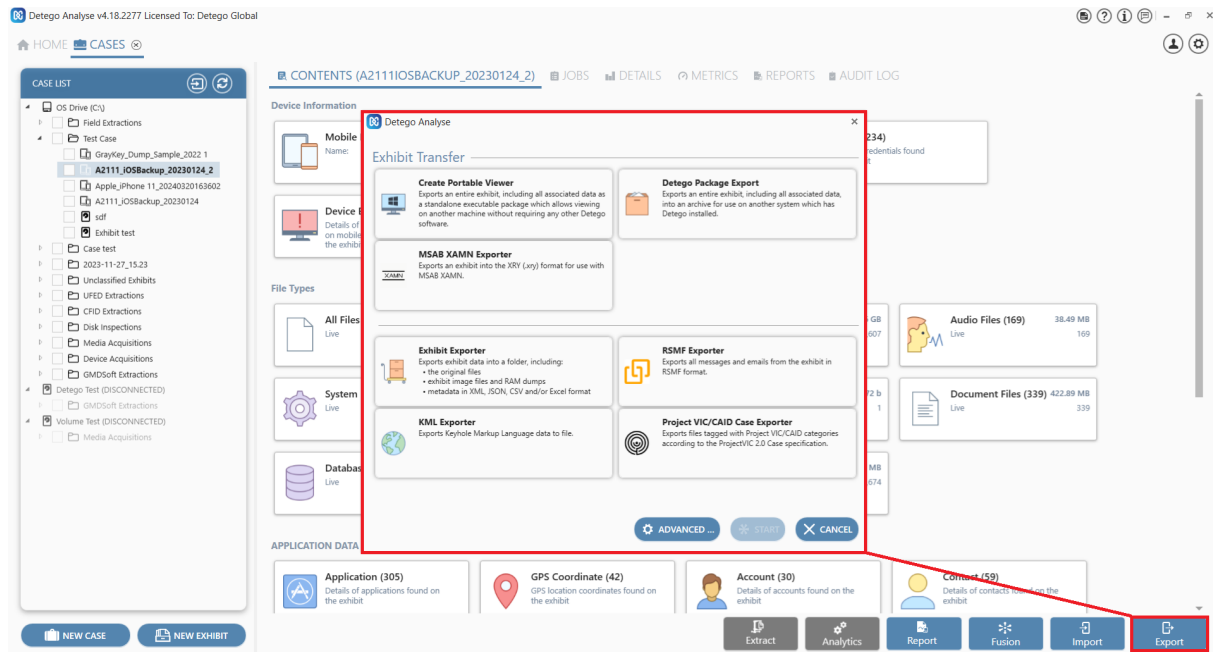
- Once the import job is done, if the AFF4 file contains a forensic image file or a physical disk image, the **Extract button** will be enabled to extract the image from the AFF4 file.
- If the AFF4 file imported contained only files, the files will be imported into Detego Analyse, and further processing can be performed. The **Extract button** will be disabled in this case

6.3. EXPORTING EXHIBITS

To export an exhibit, follow these steps:

- Select the exhibit you want to export by ticking the checkbox beside its title. To select more than one, hold down the 'shift' button whilst you click.
- Click the 'Export' button in the bottom right corner of the 'Cases' screen to open a pop-up with three [3] exhibit transfer options:

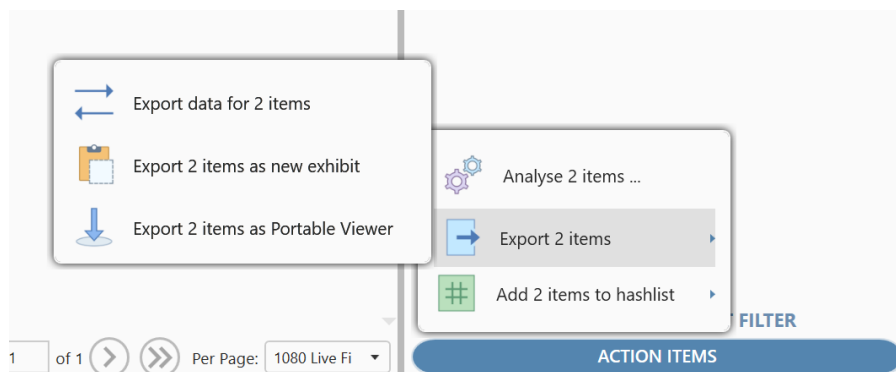
Figure 409



You can now interactively select a range of items or use a filter to define a subset of files. Then, you can export them as a new and independent exhibit or a Portable Viewer exhibit.

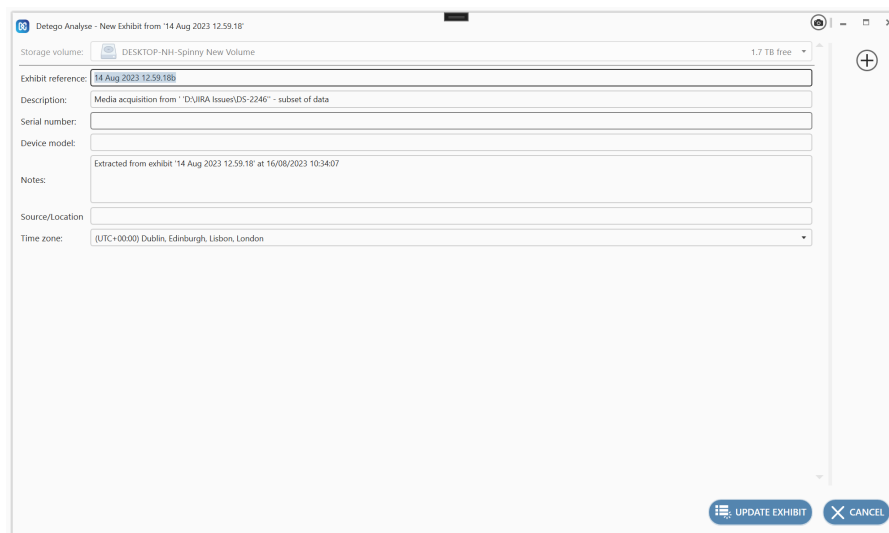
The 'Action' menu at the bottom-right of the browser window has been extended with a new context menu containing the additional options:

Figure 410



The original 'Export items' option has been moved into the menu but performs the same function. The new 'Export items as new exhibit' option brings up the new exhibit dialog with an auto-generated exhibit name and some additional messages to indicate that the exhibit was extracted from a previous one:

Figure 411



The screenshot shows a window titled 'Detego Analyze - New Exhibit from "14 Aug 2023 12:59:18"'. It contains several input fields: 'Storage volume' (DESKTOP-NH-Spinny New Volume, 1.7 TB free), 'Exhibit reference' (14 Aug 2023 12:59:18), 'Description' (Media acquisition from "D:\JIRA Issues\DS-2246" - subset of data), 'Serial number', 'Device model', 'Notes' (Extracted from exhibit "14 Aug 2023 12:59:18" at 16/06/2023 10:34:07), 'Source/Location', and 'Time zone' (UTC+00:00) Dublin, Edinburgh, Lisbon, London). At the bottom right are 'UPDATE EXHIBIT' and 'CANCEL' buttons.

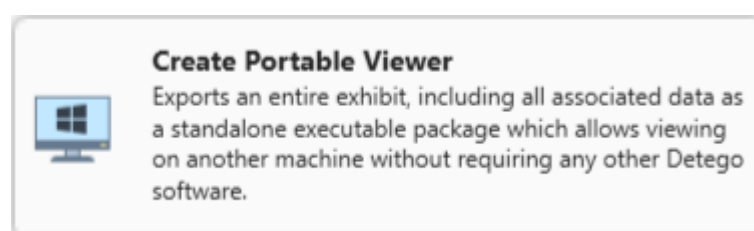
When the user clicks **EXTRACT EXHIBIT**, a new exhibit is created with only the selected (or filtered) items.

The new 'Export **n** items as Portable Viewer' option brings up the normal Portable Viewer export dialog but only exports the selected (or filtered) items.

CREATE PORTABLE VIEWER

This will create a Portable Viewer export. See the Portable Viewer section.

Figure 412



- Firstly, type in the file path in the 'Create In' box OR select the button on the right and navigate to where you want to save the package.

Figure 413

Detego Analyse

Create Portable Viewer

Create In : Please select a folder in which to create the Portable Viewer tool

Reviewer : Please enter the reviewer's name here Password : Enter password here

☒ Include Reports in Portable Viewer

☒ Include Audit Trail in Portable Viewer

☒ Include Warning Message that Examination may contain restricted content-

Options :

☒ Include Portable Viewer program with output file

Required for first export to any reviewer. Turn off to improve export time.

Please enter any notes for the reviewer here

Notes :

• Output folder missing

• Restricted content description missing

• Reviewer name missing

• Password missing

DONE CANCEL

- Once you have selected where to save the package export, type in the Reviewer's name (person designated for) and a password you wish to use if you would like to password-protect the portable viewer exhibit.

Please Note! A password is required if the "Restricted Content" toggle is switched on.

Figure 414

Detego Analyse

Create Portable Viewer

Create In : Please select a folder in which to create the Portable Viewer tool

Reviewer : Please enter the reviewer's name here Password : Enter password here

Options :

- ☒ Include Reports in Portable Viewer
- ☒ Include Audit Trail in Portable Viewer
- ☒ Include Warning Message that Examination may contain restricted content-
- ☒ Include Portable Viewer program with output file
Required for first export to any reviewer. Turn off to improve export time.

Notes : Please enter any notes for the reviewer here

• Output folder missing
• Restricted content description missing
• Reviewer name missing
• Password missing

DONE CANCEL

- Select if you want any toggle button Options on or off (by default, they will all be switched on). See the details below for what each option does:
 - **Include Reports in Portable Viewer** – Allows the ability to see reports in the Portable Viewer
 - **Include Audit Trail in Portable Viewer** – Allows the ability to see the audit trail in the Portable Viewer
 - **Include a Warning Message that Examination may contain restricted content** – This allows you to select if the exhibit contains restricted content and, if so, include a warning message for examiners.
 - **Include the Portable Viewer program with the output file** – The Portable Viewer Installer will be exported along with the exhibit. This is required for the first export to any reviewer, but we recommend leaving it on in most cases.
- If you have switched on the Restricted Content toggle, you must select from the dropdown or type in a warning message for your examiners.

Figure 415

Detego Analyse

Create Portable Viewer

Create In: Please select a folder in which to create the Portable Viewer tool

Reviewer: Please enter the reviewer's name here Password: Enter password here

☒ Include Reports in Portable Viewer

☒ Include Audit Trail in Portable Viewer

☒ Include Warning Message that Examination may contain restricted content-

Options: RESTRICTED

Required for first export to any reviewer. Turn off to improve export time.

Please enter any notes for the reviewer here

Notes:

- Output folder missing
- Restricted content description missing
- Reviewer name missing
- Password missing

DONE CANCEL

- Insert any notes for the Reviewer in the 'Notes' section and then select Done.

DETEGO PACKAGE EXPORT

This will create a Detego Package export, which is useful to archive cases for backups.

MSAB XRY EXPORTER

This will create an export of an exhibit into the XRY (.xry) format for use with MSAB forensic tools.

KML EXPORTER

The KML Exporter (Keyhole Markup Language) exports to a .kml file, which can be opened within various free-source mapping software.

Figure 416

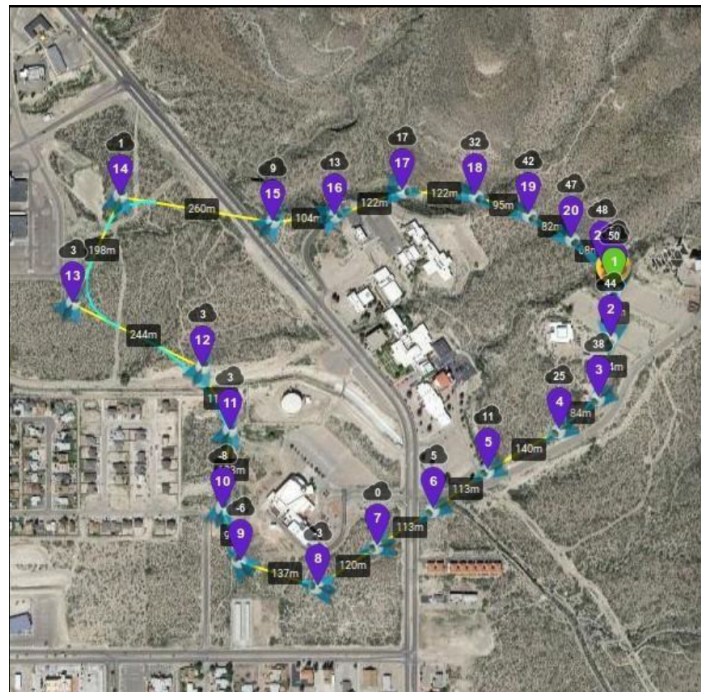
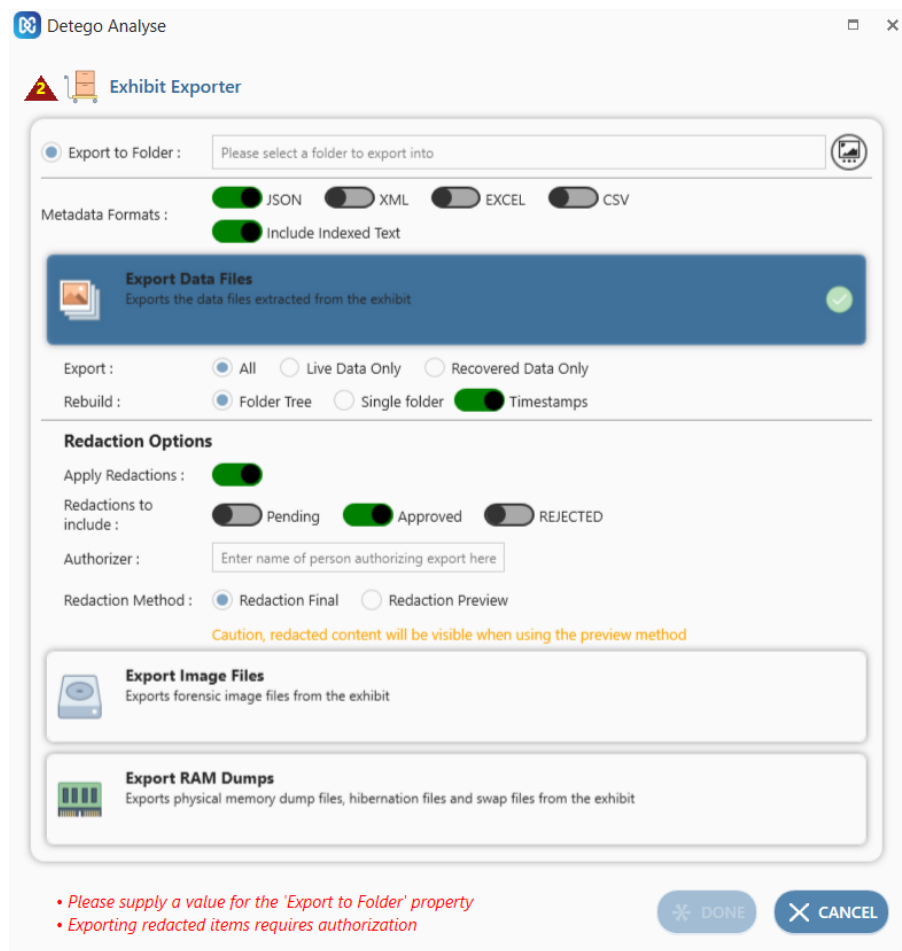


EXHIBIT EXPORTER

Creates a JSON, XML, Excel or CSV formatted export of exhibit data, with the option of including the original files.

Figure 417



Options for an Exhibit Export:

- Click the folder exploration icon in the top right corner of the pop-up to navigate to the specific empty folder where you would like the exported exhibit stored.
- 'Include Indexed Text' - This will export any indexed/translated text.
- The 'Export Data Files' button is ticked by default.
 - Select whether you would like to export 'All', 'Live Data Only' or 'Recovered Data Only'.
 - Select how you would like to Rebuild the Exhibit; either as a Folder Tree or a Single Folder.
 - Select Timestamps if you would like to export the Timestamps as well.

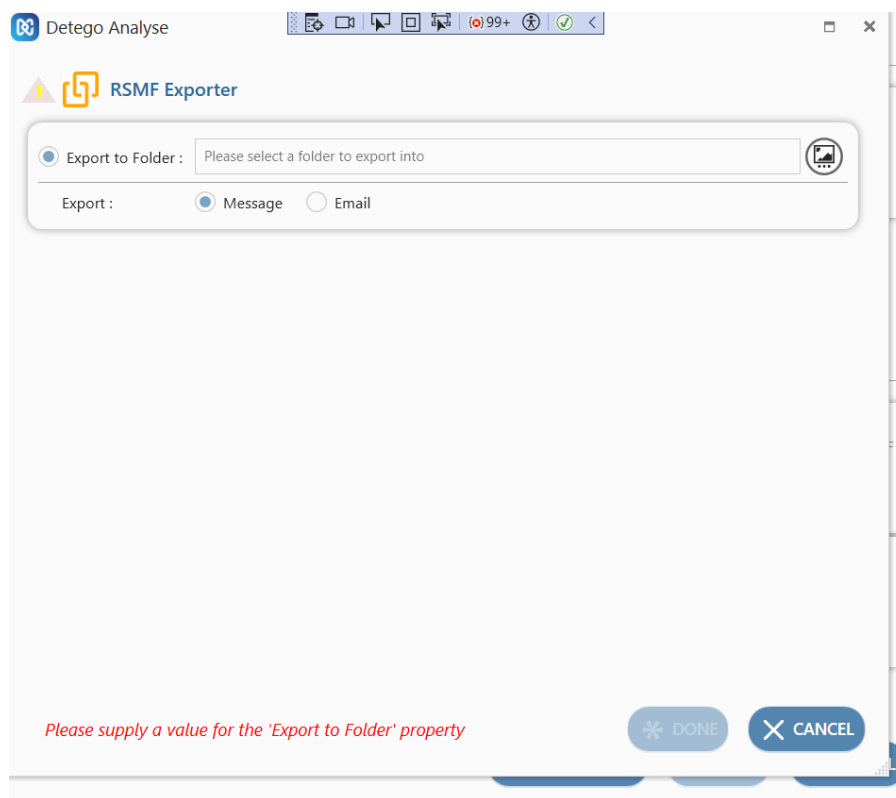
- Select whether you wish to export any redacted items and include an Authoriser if toggled on.
 - Select which redactions to include which are Pending, Approved and REJECTED.
 - Enter the name of the person authorising the export in the 'Authorizer' text box.
 - Select which Redaction Method you will use, either Redaction Final or Redaction Preview.
- You can select to include the Export Image Files which will export the files into the format they were rebuilt.
 - The Image File format that is exported will be the same as the one it was imported/rebuilt as. (E01, DD or Ex01)
- Export RAM Dumps tasks within this window to export those items if applicable.
- When you have made your selection, select DONE to start the process.

RSMF EXPORTER

Relativity Short Message Format (RSMF) is a specialised file format used within Relativity, a popular e-discovery and document review platform. The format is designed to capture and represent short message communications, such as chats and text messages, in a standardised way, allowing legal teams to review and analyse these communications efficiently during legal discovery processes

RSMF Exporter -Exports all messages and emails from the exhibit in RSMF format. it generates an RSMF file for each conversation.

Figure 418



DATABASE BACKUP

To transfer exhibits between machines via an external storage volume.

Limitations:

- The external volume must have a minimum capacity of 100GB
- User-created tags will NOT migrate
- Ensure the external volume you intend to transfer exhibits and cases is selected in the upper right before extracting/analytics.

Figure 419



- Existing exhibits can be moved to an external storage volume by right-clicking the exhibit in the CASE LIST and then selecting 'Move Exhibit ...'.
- On the pop-up, select the storage volume in the dropdown you wish to move the exhibit to from the pop-up.

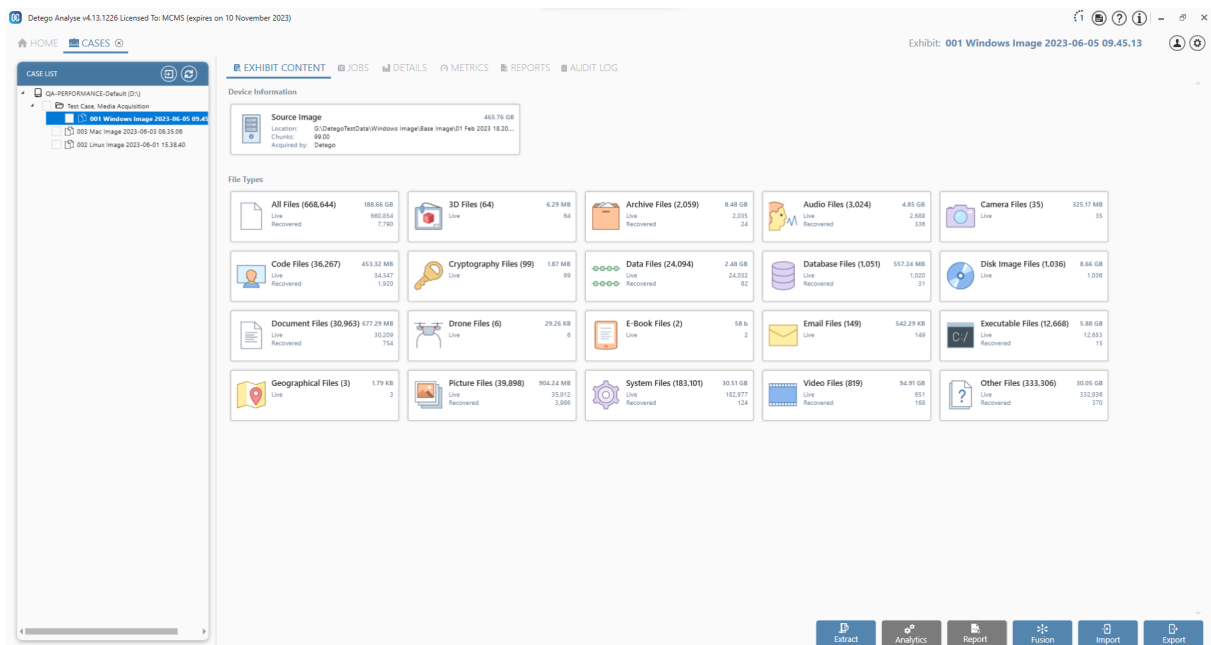
Figure 420



6.4. THE CASE MANAGEMENT HOME SCREEN

The Case Management home screen features six [6] tabs along the top of the window for providing an overview of the exhibit. These are:

Figure 421



- Exhibit content** – All of the exhibit's content groups associated with the selected exhibit will be visible

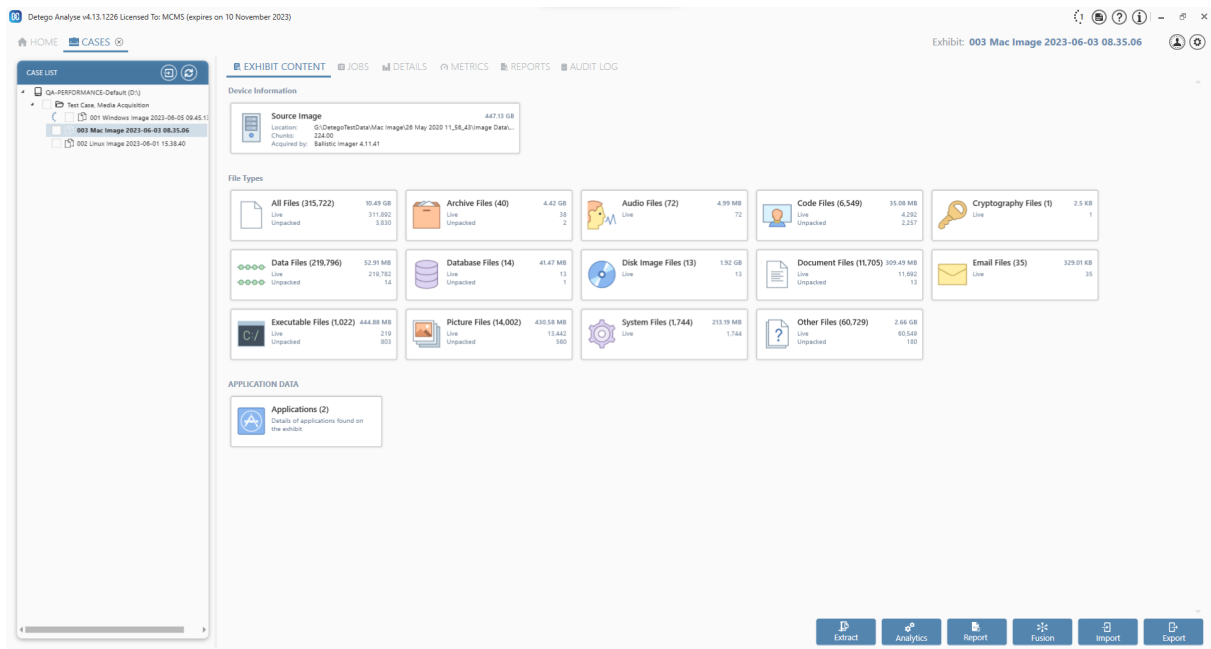
- **Jobs** - Chronologically lists the acquisitions, and analytical processes run against the exhibit.
- **Note:** This column will appear blank if no processes have been run.
- **Details** - Displays the metadata associated with the exhibit and various job statistics.
- **Metrics** - Provides a visualisation of the storage, timings, categorisation, analysis artefacts, file types and keyword matches for the exhibit.
- **Reports** - Houses all reports generated by Detego for the exhibit.
- **Audit Log** - Viewing an automated, step-by-step log across all case and exhibit actions.

At the bottom of the Case Management screen are six [6] additional actions. These are:

- **Extract** - Opens the extraction pop-up for the operator to conduct an acquisition.
- **Analytics** - Opens the analytics pop-up for the operator to conduct analytical processes against the selected exhibit.
- **Report** - Opens the reports popup for the operator to generate reports against the selected case and related file listings of acquired data.
- **Fusion** - The Fusion button opens the Detego Fusion module for advanced link analysis between exhibits and cases.
- **Import** - Used to bring other data sources into Detego Analyse.
- **Export** - Used to transfer exhibit data from Detego Analyse.

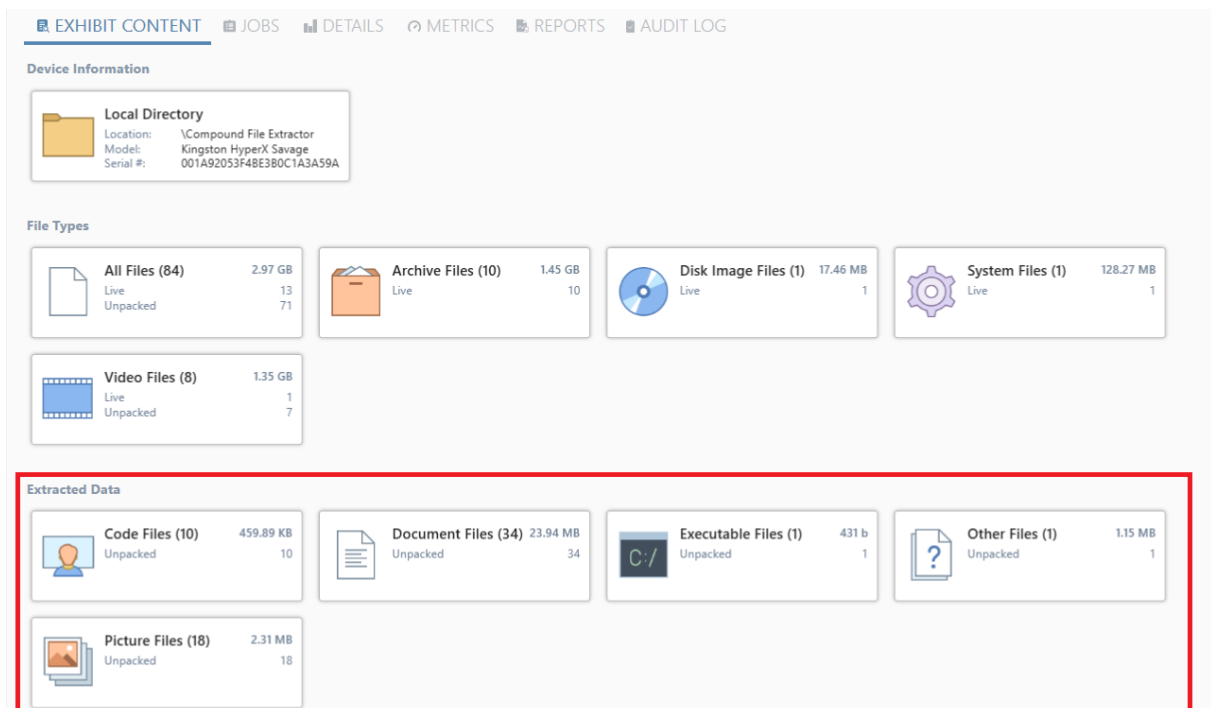
Some changes have been made to how certain data classes are stored in the database. This has enabled us to make some improvements to the way the Exhibit Contents view displays certain data classes:

Figure 422



Items extracted from compound files or documents are displayed separately on the exhibit contents buttons. Frames extracted from videos via the Video Frame Extraction job are also directly accessible and shown under 'Pictures.'

Figure 423



Additional menu items are also available when viewing files extracted from archives or videos, allowing you to return directly to the original file.

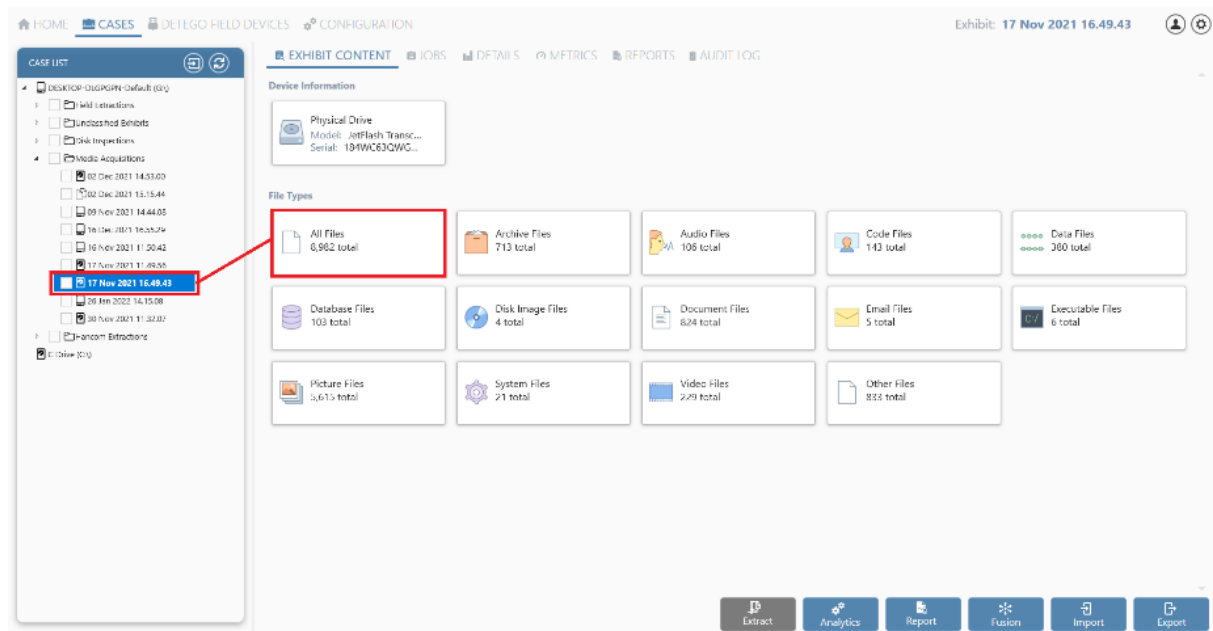
EVIDENCE BROWSER

The 'Evidence Browser' is where an investigator can view an exhibit's contents: files, pictures, database files, audio files, documents, pictures, videos, system files, app content, etc.

To access the Evidence Browser, follow these steps:

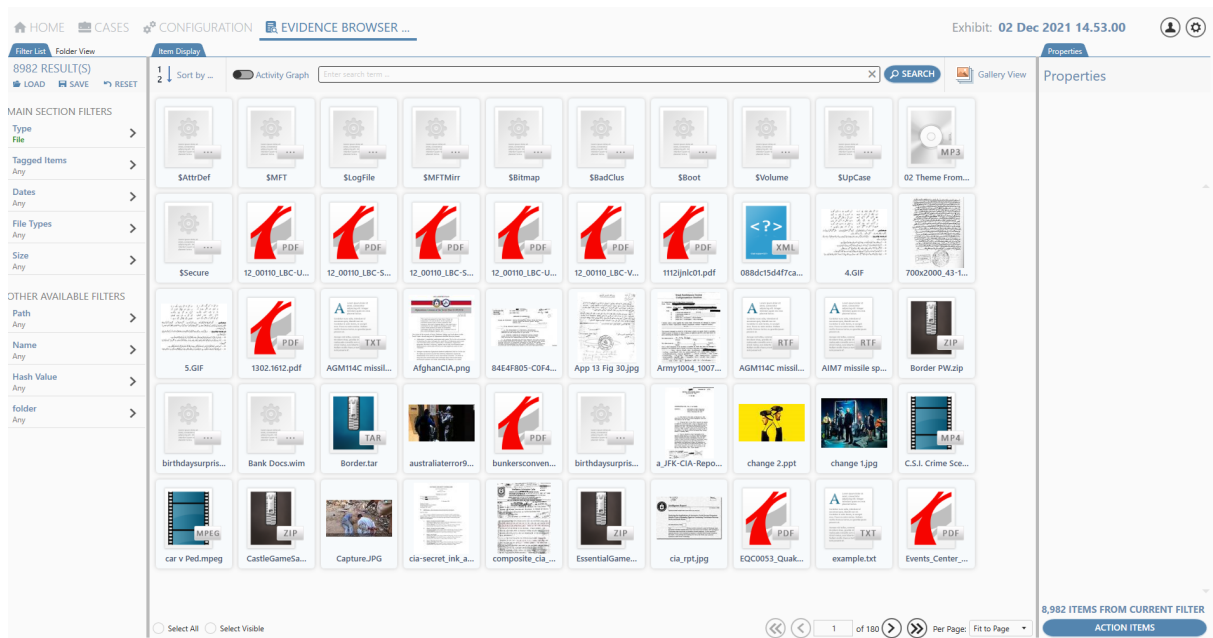
- From the Detego Analyse home screen, click the 'Analyse and Manage' tool tile.
- Select the case you want to view from the 'CASE LIST' column on the left side of the screen.
- Click the 'All files' tab from the 'Exhibit Content' tab.

Figure 424



- This will open the Evidence Browser window as shown below:

Figure 425



- All files associated with the selected exhibit are visible within the Evidence Browser window.

From here, the operator can adjust the following:

- Filter List – This shows the available filter categories you can use to adjust what is displayed in the main window. These are split into two sections.
 - Main Section Filters – This is the most common set of filters. These, by default, include: 'Type', 'Tagged Items', 'Job Reference', 'Extension', 'Size' and 'Dates'.
 - Other Available Filters – This is the second set of filters and includes by default: 'Path', 'Make', 'Model', 'Serial #', 'Folder', 'EXIF Data' and 'Hash Value'.
 - Folder View – This shows the folder structure from the exhibit and allows the investigator to navigate to a specific folder and view all files contained within that location.
 - Item Display – Displays all of the imported files and provides tools for the operator to search, sort, add filters and toggle between different viewing modes like 'Gallery View' and 'List View'.
 - Properties - Displays the file's properties, such as file name, extension, hash value, item kind, etc.

PAGE NAVIGATION

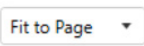
The bottom of the Evidence Browser screen shows the number of files taken from an acquisition and the number of pages to search.

Figure 426



Use the directional buttons to view different pages.

Figure 427

Arrow	Direction
	Go forward to the next page of files
	Go back to the previous page of files
	Go to the last page
	Go to the first page
	Dropdown to select how many items will be shown on one page. *This number can vary depending on your screen size and resolution

You can also navigate to a specific page by entering the page number into the page number textbox.

CURRENT SELECTION

To select files, you can manually click them and hold CTRL. As well as this, there are several options in the bottom left corner.

Figure 428

Selection	Direction
☐ Select All ☒ Select All	Select and deselect all items (CTRL+A)
☐ Select Visible ☒ Select Visible	Select and deselect all visible items (all on the current page)

Once you have selected the files you wish to target, you can run features on these files.

To do this

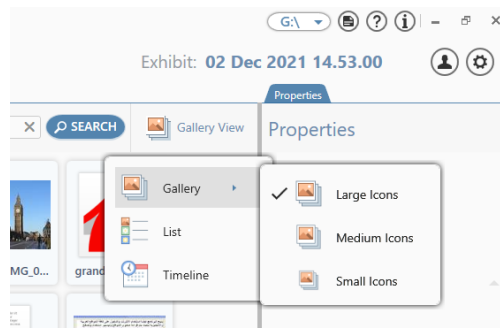
- Select files using one of the above methods
- Click the 'ACTION ITEMS' button for a popup in the bottom right corner.
- Alternatively, you can right-click one of the selected items.
- Select one of the following features.
 - Export – This feature will export all selected files to a selected destination. See the export section of the manual.
 - Analytics – This feature lets you run applicable analytics on selected files. See 14
 - Add to hash list – This feature lets you add file hashes to either a new/existing hash list. See 3.5

TOGGLING VIEW

In the 'Item Display' tab, the operator can change how the files are displayed by switching to either Gallery or List View.

- Click on the View text in the top right corner and hover over 'Gallery View' to reveal three additional icon options: Large, Medium and Small Icons.

Figure 429



- 'List View' will display the files as shown below:

Figure 430

DETEGO FIELD DEVICES CONFIGURATION EVIDENCE BROWSER ... Exhibit: 17 Nov 2021 16.49.43

Item Display Sort by ... Activity Graph Enter search term ... SEARCH List View Properties

TAGS	NAME	FOLDER	SIZE	ITEM KIND	MODIFIED	MD5	ACCESSED	CREATED
	\$AttDef	0x38	2.5 KB (2,560 bytes)	Other	22 Feb 2019 17:36:59 (UTC)	ad517ac39089580e35eac3...	22 Feb 2019 17:36:59 (UTC)	22 Feb 2019 17:36:59 (UTC)
	\$BadClus	0x38	0 b (0 bytes)	Other	22 Feb 2019 17:36:59 (UTC)	641d8cd98f020204e8009...	22 Feb 2019 17:36:59 (UTC)	22 Feb 2019 17:36:59 (UTC)
	\$MFTMirr	0x38	4 KB (4,096 bytes)	Other	22 Feb 2019 17:36:59 (UTC)	f550670d8b0b02104c69e...	22 Feb 2019 17:36:59 (UTC)	22 Feb 2019 17:36:59 (UTC)
	\$Boot	0x38	8 KB (8,192 bytes)	Other	22 Feb 2019 17:36:59 (UTC)	ead254cda833448349b71...	22 Feb 2019 17:36:59 (UTC)	22 Feb 2019 17:36:59 (UTC)
	\$Bitmap	0x38	235.38 KB (241,024 bytes)	Other	22 Feb 2019 17:36:59 (UTC)	5d77b2f0e633405fb0b69...	22 Feb 2019 17:36:59 (UTC)	22 Feb 2019 17:36:59 (UTC)
	\$LogFile	0x38	12.92 MB (13,549,568 bytes)	Other	22 Feb 2019 17:36:59 (UTC)	b58468330b6c6546e110...	22 Feb 2019 17:36:59 (UTC)	22 Feb 2019 17:36:59 (UTC)
	\$MFT	0x38	10.25 MB (10,747,904 bytes)	Other	22 Feb 2019 17:36:59 (UTC)	39e67beb50377ae81f6d2...	22 Feb 2019 17:36:59 (UTC)	22 Feb 2019 17:36:59 (UTC)
	\$Secure	0x38	0 b (0 bytes)	Other	22 Feb 2019 17:36:59 (UTC)	641d8cd98f020204e8009...	22 Feb 2019 17:36:59 (UTC)	22 Feb 2019 17:36:59 (UTC)

Gallery List Timeline

FILE PROPERTIES

To view a file's properties, click on it to display it in the 'Properties' tab on the right-hand side of the Evidence Browser window or hover over it.

Figure 431

HOME CASES CONFIGURATION EVIDENCE BROWSER ... Exhibit: 02 Dec 2021 14.53.00

Filter List Folder View Item Display Graph Enter search term ... SEARCH Gallery View Properties

8982 RESULT(S) LOAD SAVE

MAIN SECTION FILTERS

Type File

Tagged Items Any

Dates Any

File Types Any

Size Any

OTHER AVAILABLE FILTERS

Path Any

Name Any

Hash Value Any

Folder Any

Select All Select Visible

1 of 180 Per Page: Fit to Page

1 ITEM IN CURRENT SELECTION ACTION ITEMS

Properties

Name device Australia1.JPG

Location 0x38\device Australia1.JPG

Folder 0x38

Size 1.55 MB (1,626,753 bytes)

Accessed 22 Feb 2019 17:42:54 (UTC)

Modified 14 Mar 2016 14:11:31 (UTC)

Created 22 Feb 2019 17:43:54 (UTC)

MD5 48c2510eb8400145f4271808f02976d

SHA1 e9c11999006728ff4b031802c0a08a07e050

Extension .jpg

Item Kind Picture

File properties attributes:

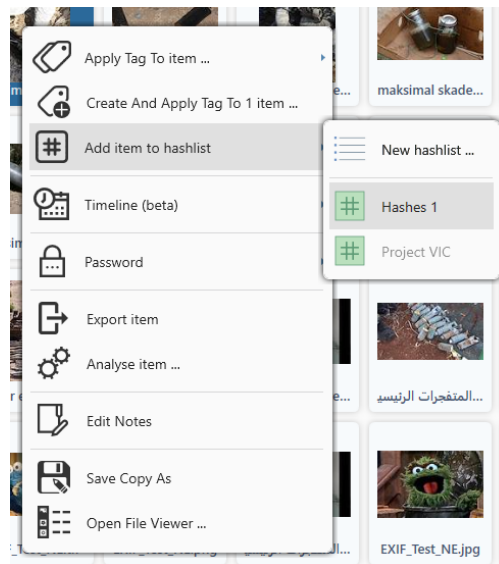
- **Name** – The name of the file as it appears in the evidence volume.
- **Size** – The size of the file in bytes.
- **Extension** – The file's extension, i.e. .jpg
- **Location** – The file's folder location
- **SHA1/MD5** – The hash value of the selected file, either in SHA1 or MD5.
- **Created** – The time the file was created on the evidence volume.
- **Folder** – The folder in the evidence volume in which the file was residing.
- **Item Kind** – The categorisation of the file, e.g., picture, document, etc.
- **Modified** – The time the file content was last changed and then saved on the evidence volume.
- **Accessed** – The time the file was last touched on the evidence volume.
- **Is Deleted** – Whether or not it was a deleted file acquired by carving.
- **Job Name** – The name of the Detego Analyse job that extracted the file and the extraction date, e.g., Logical Extraction.

ADDING TO HASHLISTS

Adding to or creating hashlists from within the evidence browser.

- From within the Evidence Browser – highlight or select the files whose hashes you wish to add to an existing hashlist or a new hashlist.
- Right-click any selection member and select "Add X items to hashlist."
- Either add to existing hashlists as displayed or Add to a New hashlist

Figure 432

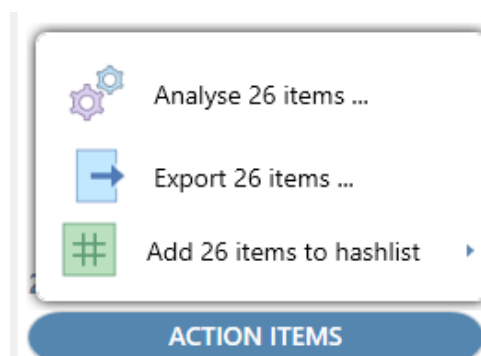


Alternatively

From within the Evidence Browser:

- Highlight or select the files whose hashes you wish to add to an existing hashlist or a new hashlist.
- Click the 'ACTION ITEMS' button in the lower right corner.
- Select "Add X items to hashlist."
- Either add to existing hashlists as displayed or Add to a New hashlist.

Figure 433



6.5. DETEGO OMNIVIEWER

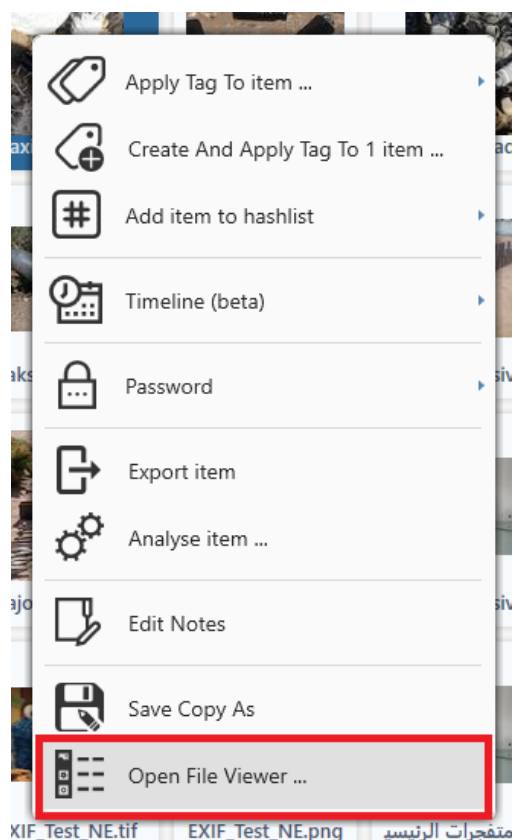
Double-click on a file from the Evidence Browser to open the 'Detego Omniviewer'.

Figure 434



This can be accessed by right-clicking the file and clicking 'Open File Viewer'.

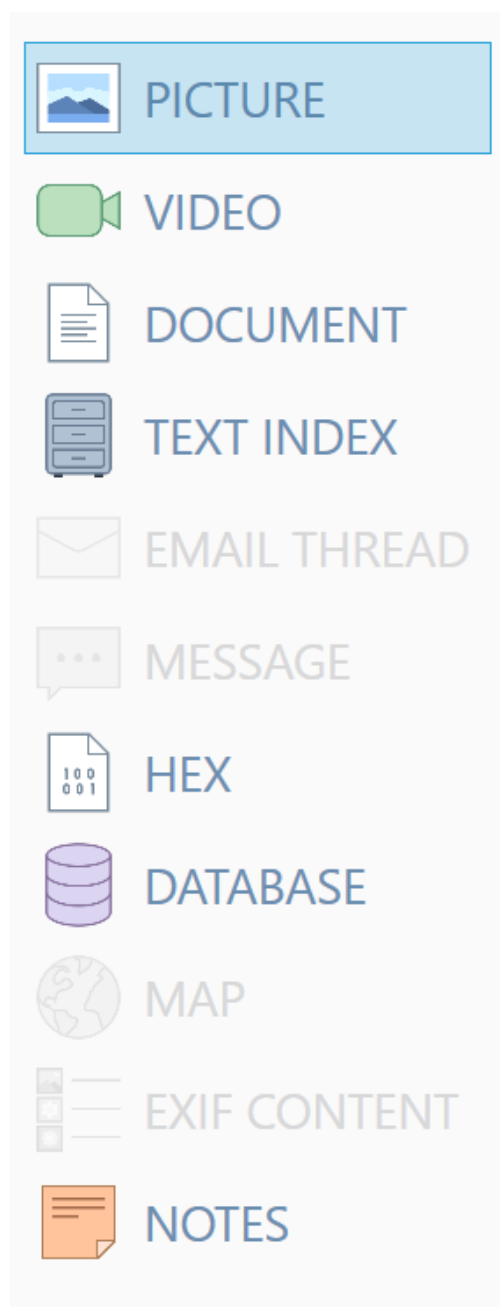
Figure 435



The Detego Omniviewer will automatically open up the most relevant file item in the Omniviewer's sub-screen, e.g., a .png file will open under the 'Picture' tab.

Text and logos for the unavailable options will be greyed out when the omniviewer loads.

Figure 436



The options on the left of the pop-up are as follows:

PICTURE

Displays images. The operator can zoom the picture by moving their mouse over it to use the magnifying glass function or click on the icon to the left of the window. The rotational icons rotate the image clockwise or counter-clockwise, respectively.

Figure 437

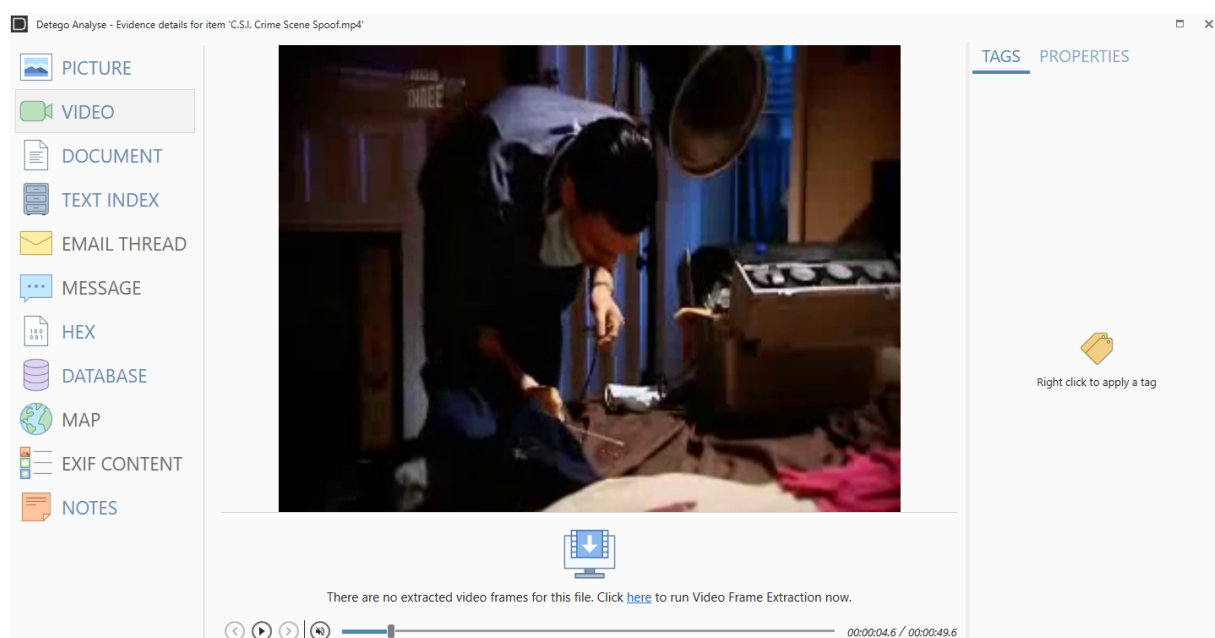


The column on the right of the pop-up details any tags which have been applied (right-clicking here also allows the application of any new tags, as required) and the file's properties.

VIDEO

Displays video or audio files. Click the play icon at the bottom of the screen to run the item, the arrow icons to skip, and the volume icon to adjust the sound levels.

Figure 438

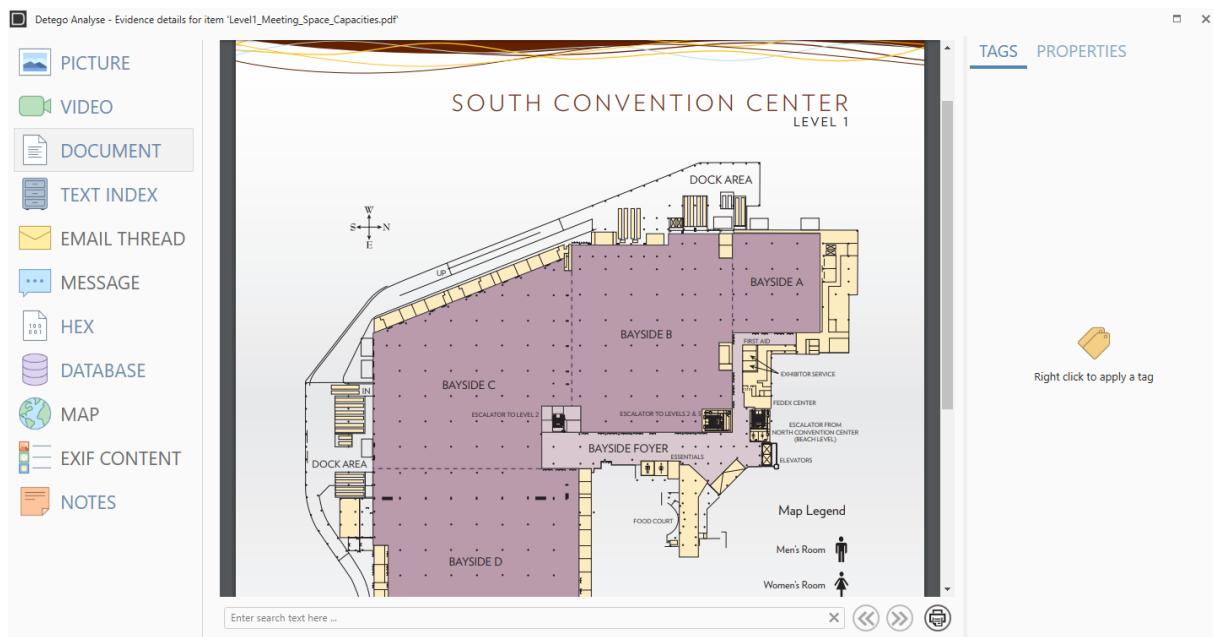


The column on the right of the pop-up details any tags which have been applied (right-clicking here also allows the application of any new tags, as required) and the file's properties.

DOCUMENT

Displays document files. The operator can scan the document for a particular search by typing it into the field at the bottom of the screen. For multiple matches of searched text, they can click the directional arrows to the left and right of the search bar to find the next or previously found term and toggling 'Match Case' on will look for text in a case-sensitive mode. To print the document, click the printer icon in the bottom right corner of the window.

Figure 439

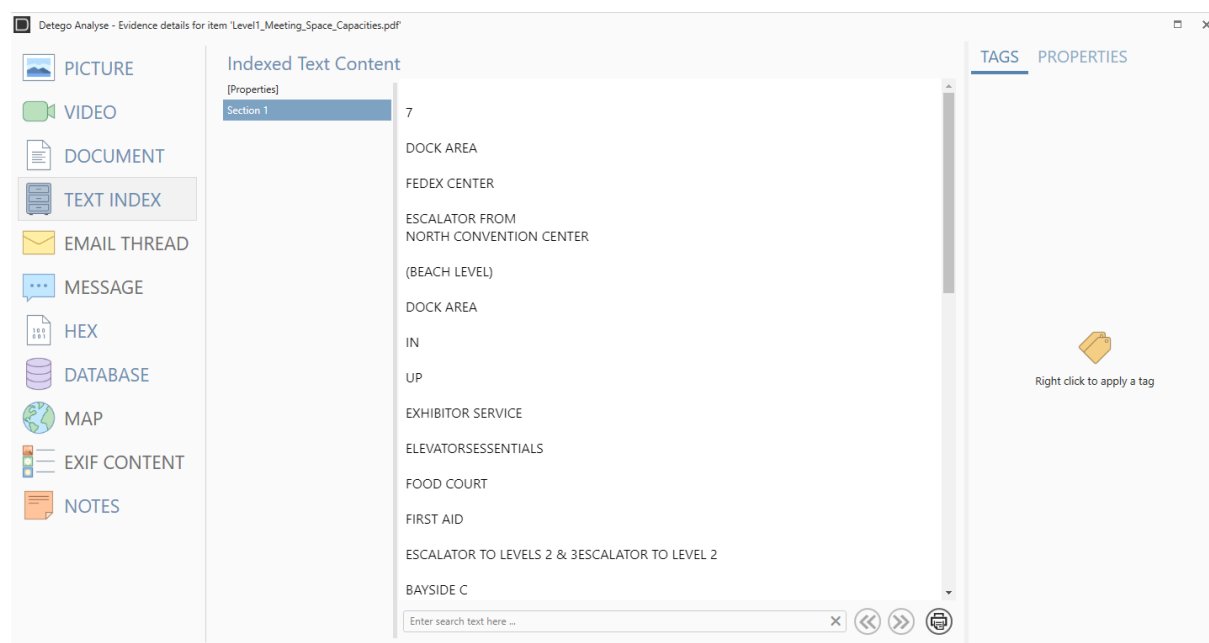


The column on the right of the pop-up details any tags which have been applied (right-clicking here also allows the application of any new tags, as required) and the file's properties

TEXT INDEX

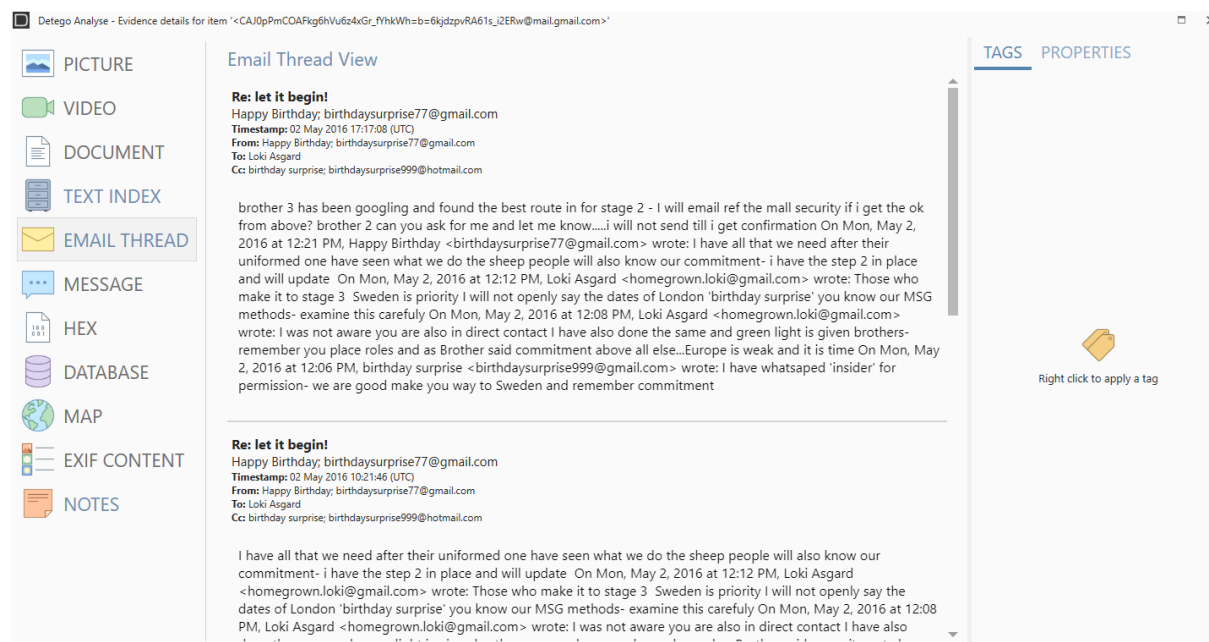
Displays the basic information of the file, including the MD5 and SHA1 Hashes. Once the Text Indexer job has been run on the item, you can view the indexed text within the separate sections.

Figure 440



'Email Thread' – Displays an email thread if available. To view this, you must run the App Parser job beforehand. Once run, you can view the items from 'Emails' in the Exhibit Content screen.

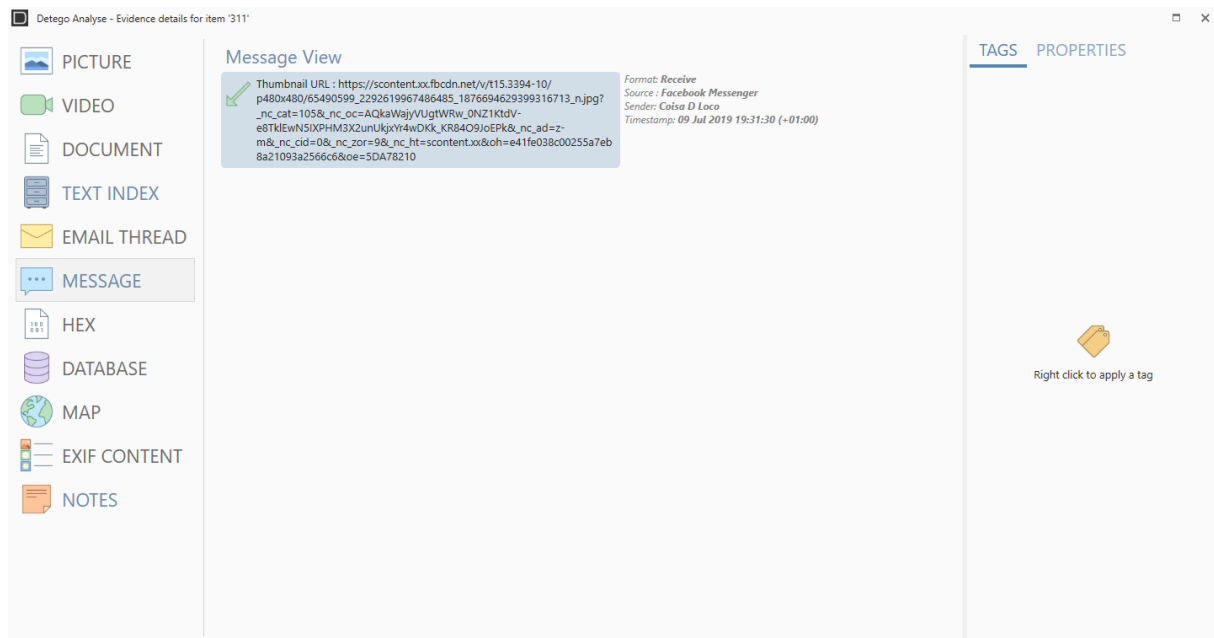
Figure 441



MESSAGE

Displays messages extracted from mobile devices.

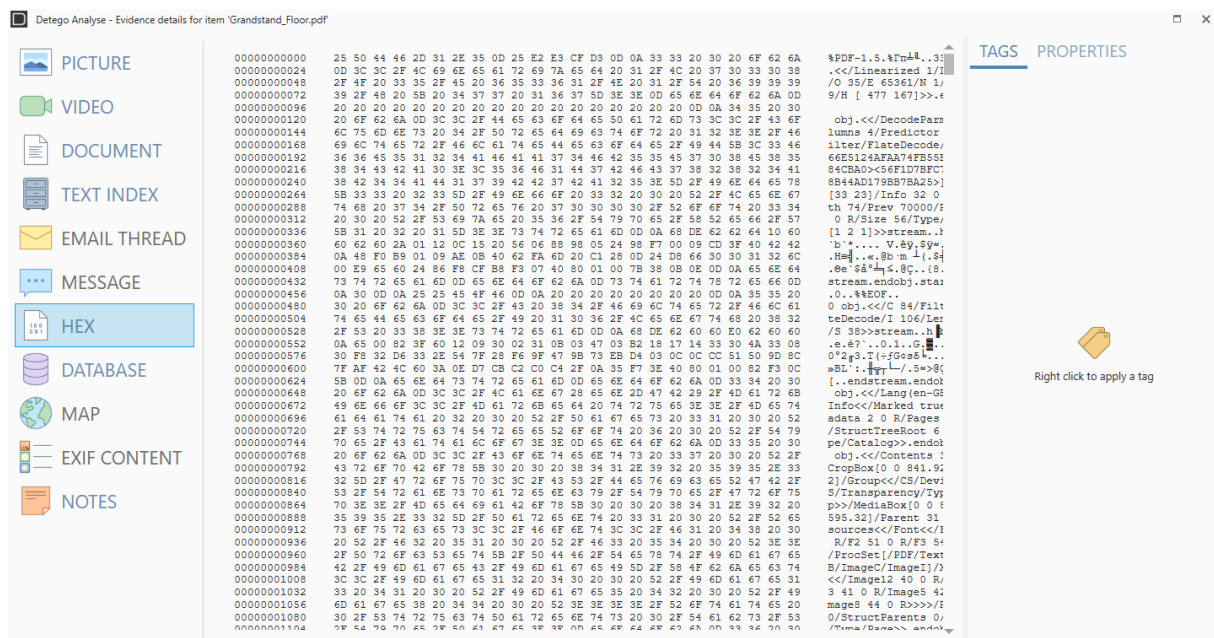
Figure 442



HEX

Displays all the binary data attached to the file.

Figure 443

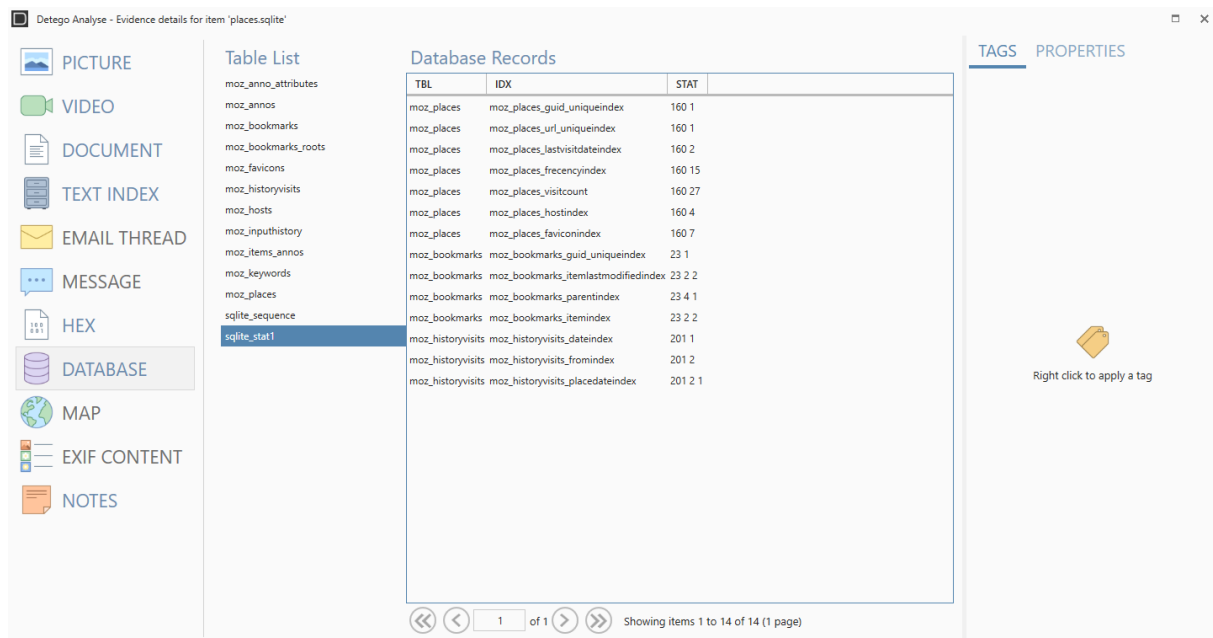


The column on the right of the pop-up details any tags which have been applied (right-clicking here also allows the application of any new tags, as required) and the file's properties

DATABASE

Displays SQLite databases. The 'Table List' shows all the tables inside the database, and the 'Database Records' column shows the data inside the table. The arrows at the bottom of the screen move the pages forward and backward.

Figure 444



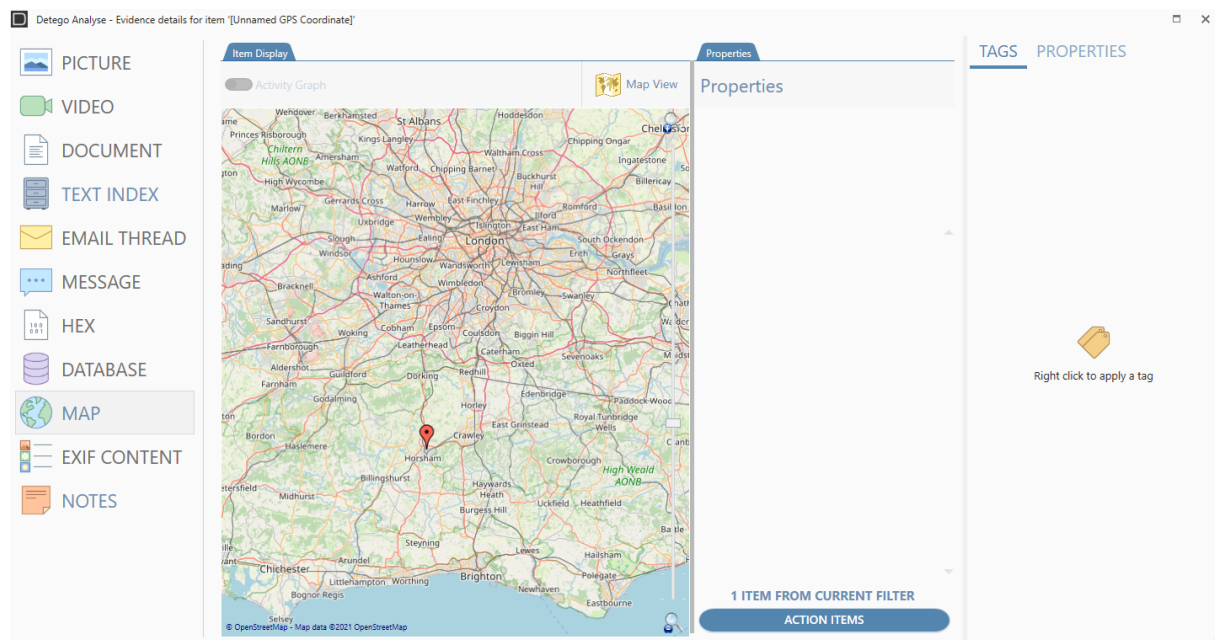
The column on the right of the pop-up details any tags which have been applied (right-clicking here also allows the application of any new tags, as required) and the file's properties

MAP

If there is any GPS-based data (typically found in picture files and data from smartphones), it will drop a flag onto a map showing the location.

Note: You need to be online to connect to the mapping software.

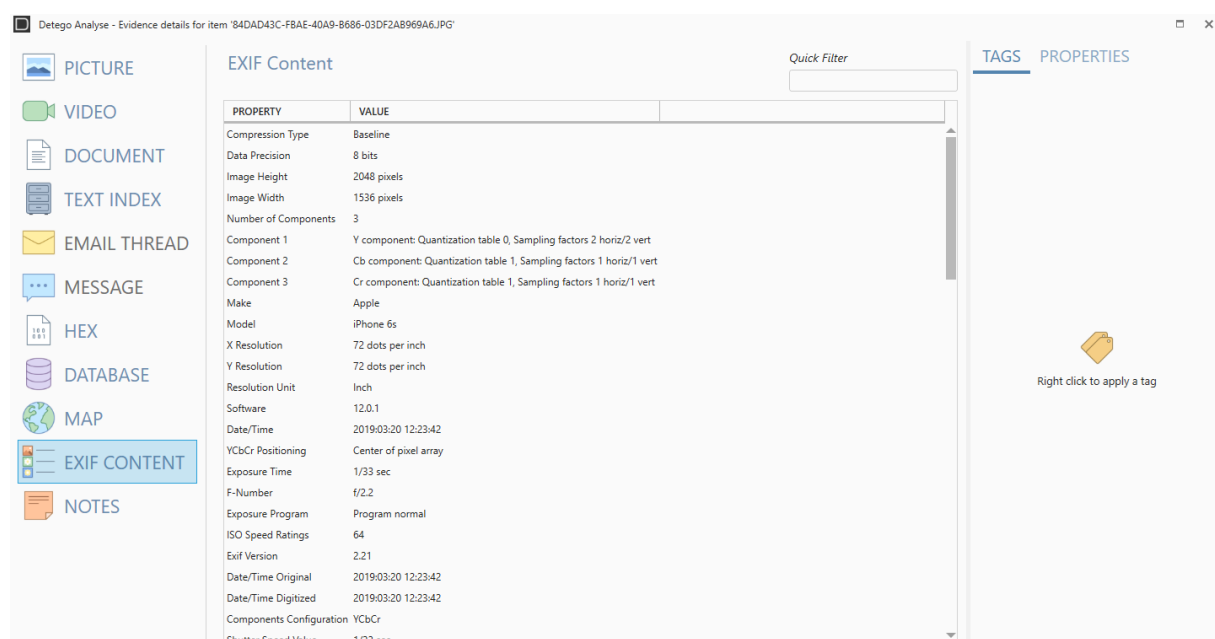
Figure 445



The column on the right of the pop-up details any tags which have been applied (right-clicking here also allows the application of any new tags, as required).

'EXIF Content' - EXIF (Exchangeable Image File) is a standard format for storing interchange information in digital photography image files using JPEG compression.

Figure 446

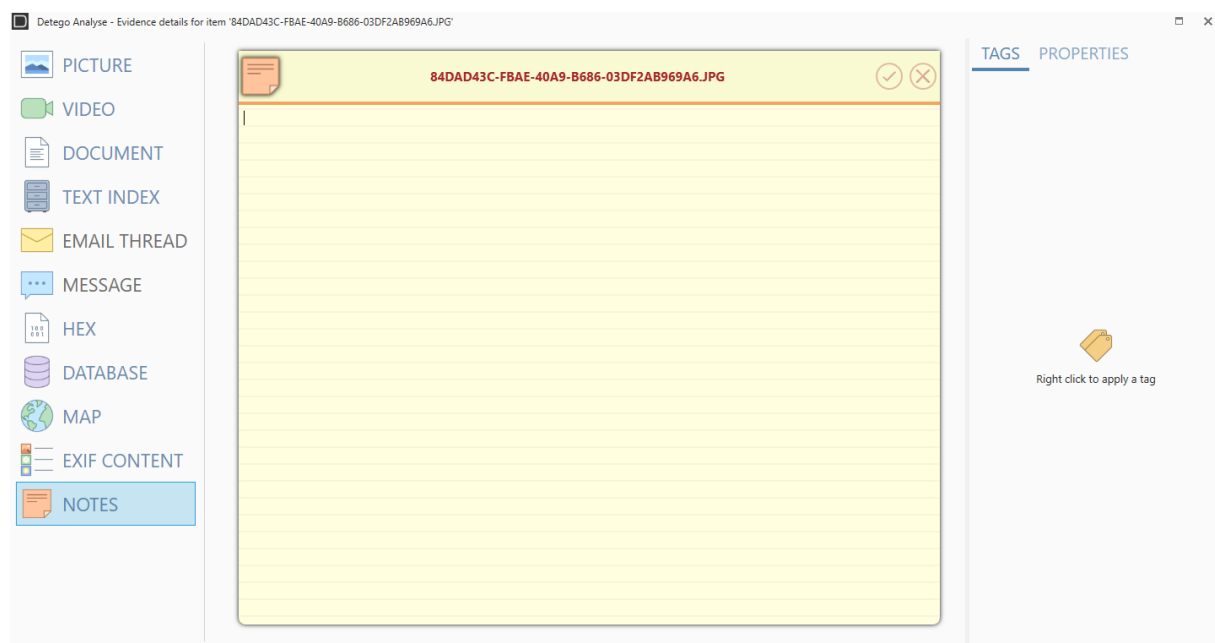


The column on the right of the pop-up details any tags which have been applied (right-clicking here also allows the application of any new tags, as required).

NOTES

From here, the operator can enter log notes against the evidence item; these will be added to the audit log and can also be added to reports. Click the tick icon in the window's top right corner to save.

Figure 447

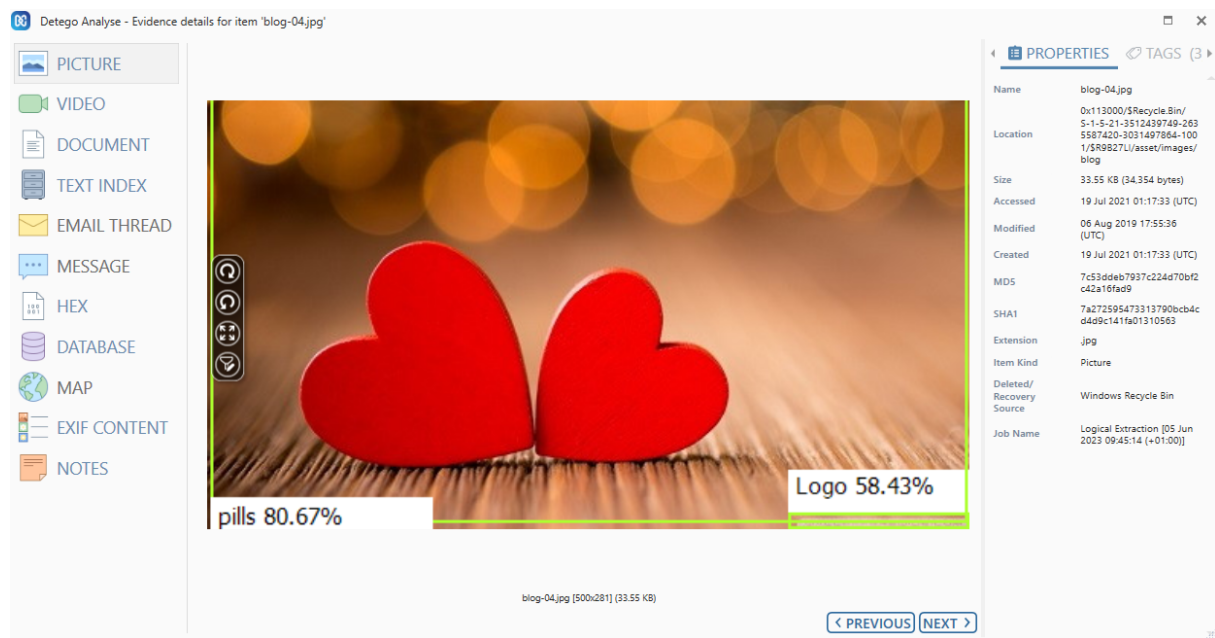


The column on the right of the pop-up details any tags which have been applied (right-clicking here also allows the application of any new tags, as required).

NAVIGATION

Users can now quickly go through files whilst staying on the Omniviewer screen. This can be achieved by selecting either button depending on which direction they would like to go. Keyboard shortcuts are also available using arrow keys, `HOME`, `END`, `PAGE UP` and `PAGE DOWN`.

Figure 448



6.6. TIMELINE VIEW

Timeline View is one of the three 'Views' in EXHIBIT CONTENT. It shows items from exhibits chronologically and clarifies items within various periods.

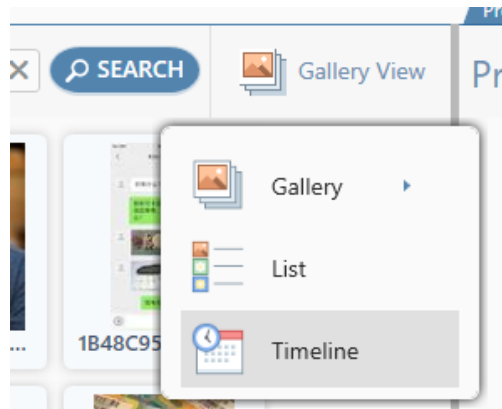
ACCESSING TIMELINE VIEW

The Timeline View can be accessed from the View Menu Dropdown in Exhibit Content.

To do this, follow the following:

- Select an exhibit and navigate to EXHIBIT CONTENT.
- In the top right corner of the content window, select the View Menu Dropdown. This usually defaults to Gallery View.
- Select Timeline from the dropdown.

Figure 449



- In addition, the Timeline summary can be shown above the other views where appropriate by clicking the 'Show Timeline' toggle on the right side of the 'Sort by ...' menu button. Any data shown in that view will be further restricted to the period identified by the grey area in the Timeline summary.

Figure 450

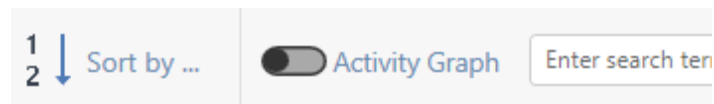
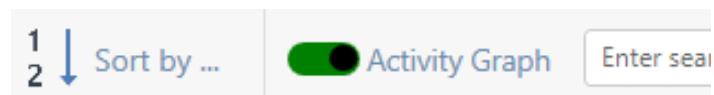
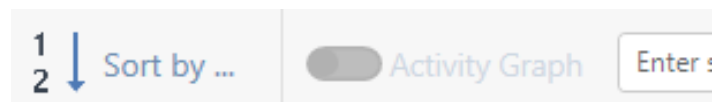


Figure 451



- The filter can then be clicked again to toggle off (hide) the time bar.

Figure 452



The toggle switch can appear disabled if none of the items returned by the left panel filters has date properties.

FILTERS

The Timeline View will honour all existing filters and search terms and react to them accordingly when they change.

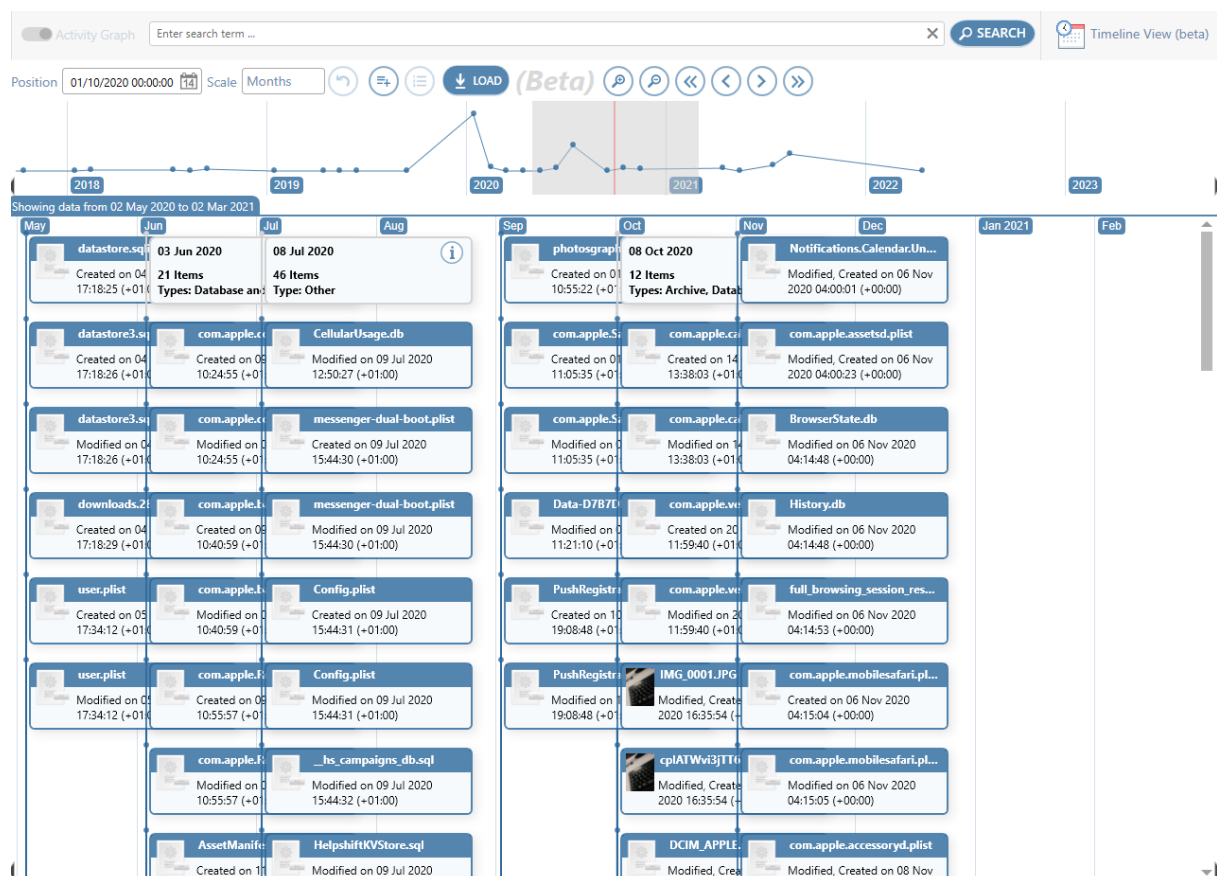
PLEASE NOTE! The 'Sort by ...' function won't be available while using Timeline View as it will always be sorted chronologically.

LAYOUT OF TIMELINE VIEW

You will see similar to the below image. The toolbar at the top of the window allows you to control the position and scale of the view.

The main panel shows items positioned based on their taggable properties (an item may appear more than once as most taggable items have multiple dates). You can see the filename and associated thumbnail in the gallery view (if applicable).

Figure 453



The small section between the toolbar and the main panel shows items as a line graph to identify areas containing items and 'busier' periods. It will have a greater scale than the main bar, which provides a quicker way of scrolling.

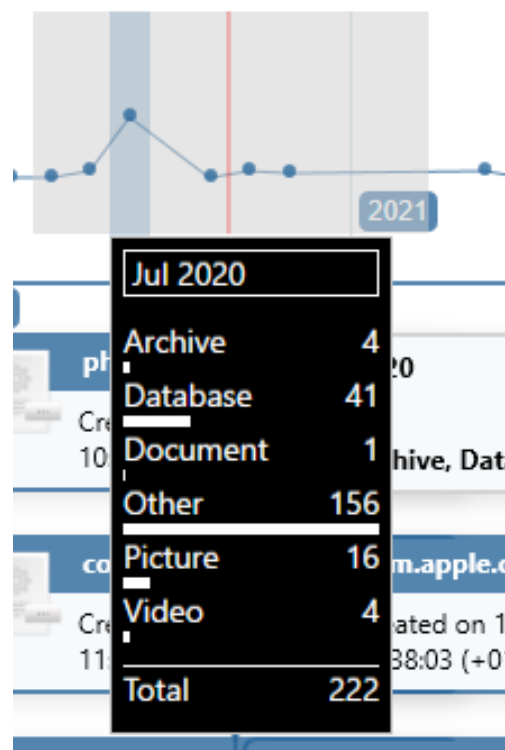
Figure 454



The width of each column in the graph is highlighted in grey when the mouse hovers over) represents the width of its relevant time slot (month, day, etc.) and will vary when zooming in and out. This means it is easier to identify when part of a slot is outside the grey viewable area. The graph point will always be shown in the middle of the column.

The bars in the summary will highlight when the mouse moves over them and will also show a tooltip with a breakdown of the contents of that time slot, as shown below.

Figure 455



The tooltip title will be the date and possible time the column represents. This may be partial, as shown above, and will depend on the current scale.

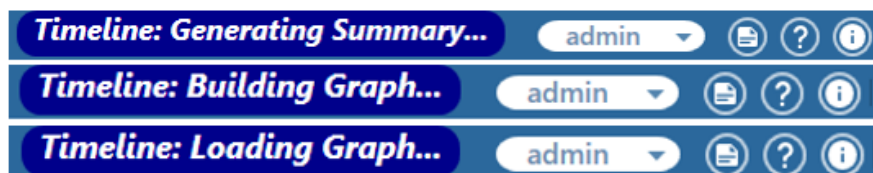
For example:

- Months: YYYY-MM
- Days: YYYY-MM-DD
- Hours: YYYY-MM-DD-HH00 (e.g., 1900 hours)

Double-clicking on a bar in the summary will drill down to the next scale with the date/time bounds as a data limit. Therefore, you can further inspect the items in a specific time scale without additional surrounding data or the need to change the traditional Analyse date filter on the left panel. See the Drilling Down section to learn more about “Drilling Down”.

The information below will be visible in the Analyse toolbar, while the main summary graph is generated for lengthy queries. The three messages may not all be displayed. They may be displayed for varying durations depending on the size of the dataset and performance spec of the machine Analyse is running on.

Figure 456



CONTROLLING THE VIEW

TIME POSITION

The Position control in the toolbar will change as the view is scrolled. In addition, the date can be set in the control to jump to any date.

Figure 457

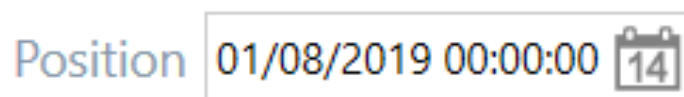


Figure 458



The four (4) arrow controls in the top right of the toolbar can be used to jump to the first, next, previous and last points of interest in the line graph. The time position will be set to that represented by the start date of the column containing a dot, so it can be quicker to scroll through the Timeline if it spreads out.

These buttons will be disabled if there are no more dots to the left or right, respectively.

You can also click a dot in the line graph, and the position will jump to that date/time.

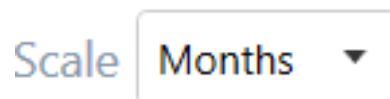
You can scroll the views by clicking and dragging the mouse in either panel. The smaller summary bar will scroll more quickly with a greater scale.

You can also scroll by swiping the mouse, which has an inertia function and slowly slows to a stop.

The main panel can be scrolled without loading any data. This is because each load could display items not in the visible area.

SCALE

Figure 459

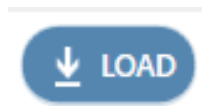


The Scale control in the toolbar can set the value of the x-axis of the main view (in the example shown above, the labels in the main panel are months). Moving to smaller time increments, such as minutes, means that items will spread further, making it easier to identify items during 'busy' periods. However, this will greatly increase the data loaded, so it is sensible to combine this move with the addition of a specific date filter to refine the results or by drilling down.

If the desired scale is absent, filter the date range on the left panel to reduce the results or double-click to the next scale down.

LOADING THE MAIN PANEL

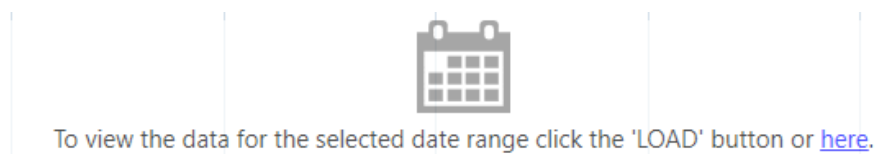
Figure 460



Once you have filtered data and navigated to a period of interest from the main time bar, you can view the items for the highlighted grey area in the main panel below it. This can be performed using the LOAD button, as shown above.

The prompt below will appear in the main panel when this is necessary. This is to differentiate between an empty panel and no results. The data can also be loaded by using the hyperlink shown.

Figure 461



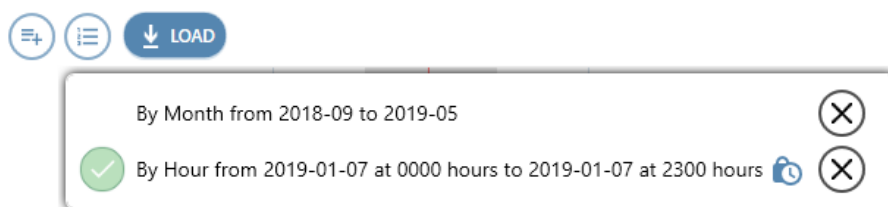
SNAPSHOTS

There are two buttons to assist with navigation. It is possible to save the current view as a snapshot and then select snapshots from a menu to navigate directly to a point in time with the scale and zoom factor present when the snapshot was saved.

Figure 462



Figure 463

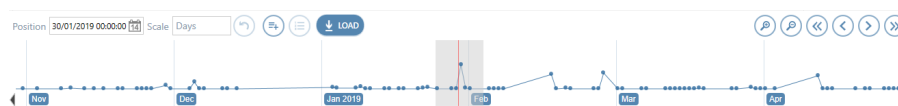


The above image is the snapshot menu to which items are added when clicking the 'Add' button. Each item shows the time position and scale that was saved. The green tick indicates the last one selected. Snapshots can be removed by clicking the cross, and the selected snapshot can be 'released' by re-selecting it. This will reload the Timeline at the same position and scale without the date restriction. Therefore, you can expand the results to include everything the left taggable filters provided.

NOTE! It is important to note that if you are currently in a date-restricted view (either by drilling down or within another snapshot), the view will only show that portion of the Timeline summary. Some navigation options, such as changing the scale, will also cause the current snapshot to be deselected, and thus the entire summary line will appear.

The example below shows that the user has manually navigated to a specific day (30th January 2019).

Figure 464



However, if the user double-clicks on January 2019 from the Months scale, the view will look like the below.

Figure 465



When selected, this will be reflected in any added snapshots and what they display in the Timeline.

Adding a snapshot at this point would disable the restricted view icon, as the snapshot now controls the timeline's date range. However, scrolling the Timeline moves the snapshot's exact date to be deselected. If the snapshot has a reduced date range, the restricted view icon will reenable, thus allowing the user to view the entire Timeline again.

Snapshots are transitory and lost when the user navigates from the evidence browser. They can, however, be permanently saved if the user saves the current filters. Any present snapshots will

be loaded back into the snapshot menu when the filters are reloaded. This means the user can easily use the same filters and Timeline to focus on multiple exhibits, aiding activity comparison.

ZOOM

There are zoom-in/out controls on the right of the toolbar.

Figure 466

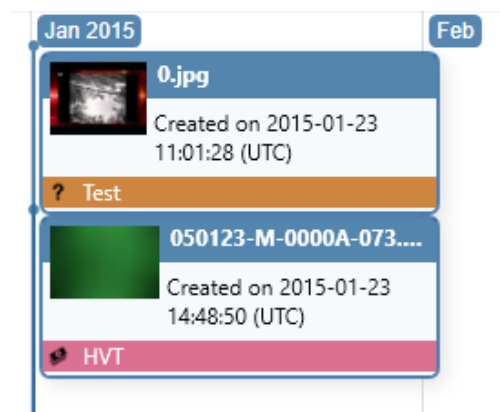


These will spread out or compress the view horizontally. Compressing the view is useful as more data will be loaded into the main area each time (because that area's start and end dates are now further apart). Spreading the view is useful during busy periods so that less data is loaded and there is less overlapping of items, so the view is clearer. You can also use the CTRL+ Mouse Wheel method to zoom in and out.

You can't zoom in further if the Timeline summary or main panel only contain two columns. At this point, the zoom-in button will be disabled.

MAIN PANEL 'FLAG' FUNCTIONS

Figure 467



The items in the main panel will respond to the same events as those in the gallery view.

- Hovering over shows further info for individual items – clicking the  button for groups.
- A single left click shows properties on the right (not for multiple items or groups).

- Double-click launches omniviewer OR navigate to the Grouped Items.
- Use CTRL + left click to select or deselect multiple items.
- Right-click for the context menu (enabling, etc., Should work the same as gallery view).
- Tags will be displayed across the bottom of the flag.

When selecting flags in the main Timeline view, it may be possible that other visible flags become selected. This is because they may represent the same artefact but with different dates. For example, if a picture was modified after creation, you may see two versions in the view. Flags represent events occurring to artefacts, not just the artefact itself.

GROUPED ITEMS

Items will be grouped into a single flag if they are close in terms of date (relative to the current scale) and more than ten items.

Figure 468

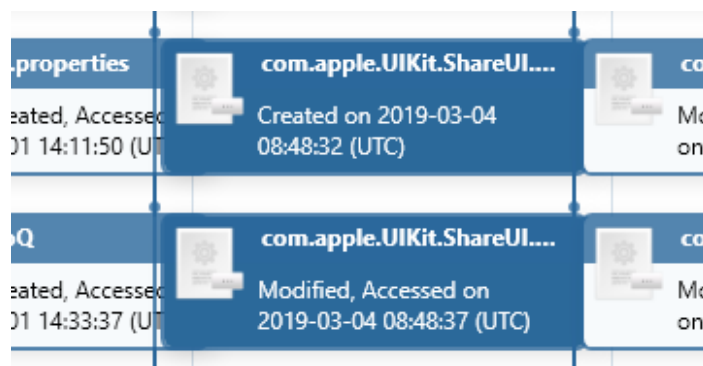
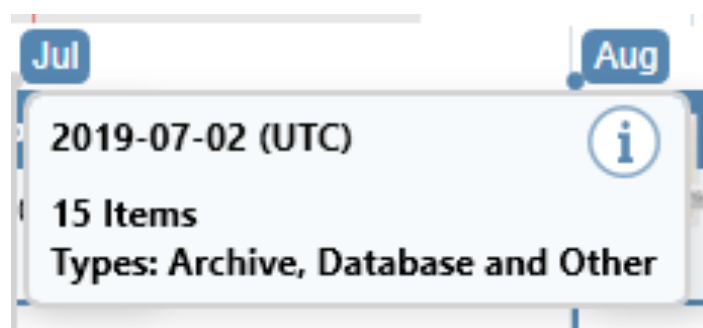


Figure 469



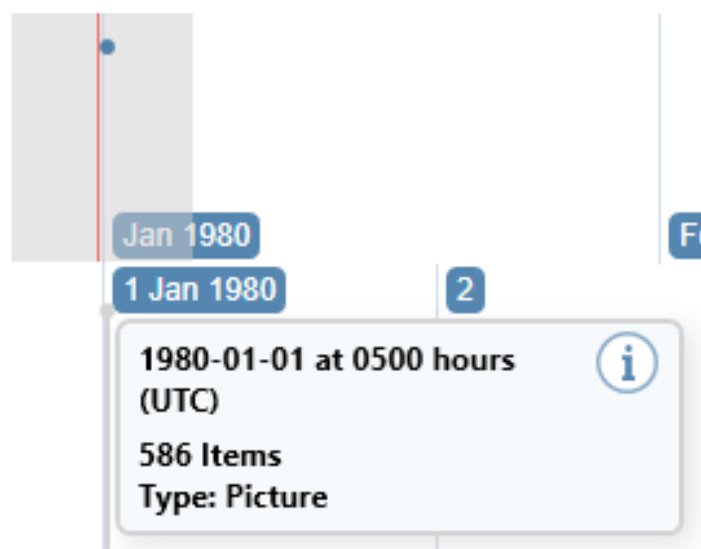
The above example shows 15 items, all on 2nd July 2019. As we are in the month view, the grouping uses days to group by. The items are a mixture of three types listed in the description.

Selecting such a group will select all of the items within. You can use CTRL + left click to deselect them as well. There may also be single items and, indeed, other groups.

DRILLING DOWN

As mentioned briefly, double-clicking a group will show the Timeline for **that group only**, making the Timeline a lot shorter and with less data but more detail on the group. You may even find that the line graph at the top has only one dot, as below.

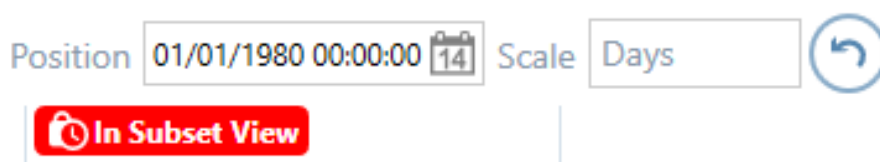
Figure 470



Since we have gone 'into' a group, the scale is reduced, so we are now on Days (1st January 1980). The items are still grouped. They are all within the same hour and still more than ten items. You can continue double-clicking groups until you get to the millisecond scale. If there are still groups, they may have the same time.

Using the Scale control will move you back up through the process above, limiting the view to the smaller dataset. When you reach the scale where the first double-click occurred, the restriction will be removed, and you will see the entire Timeline again.

Figure 471

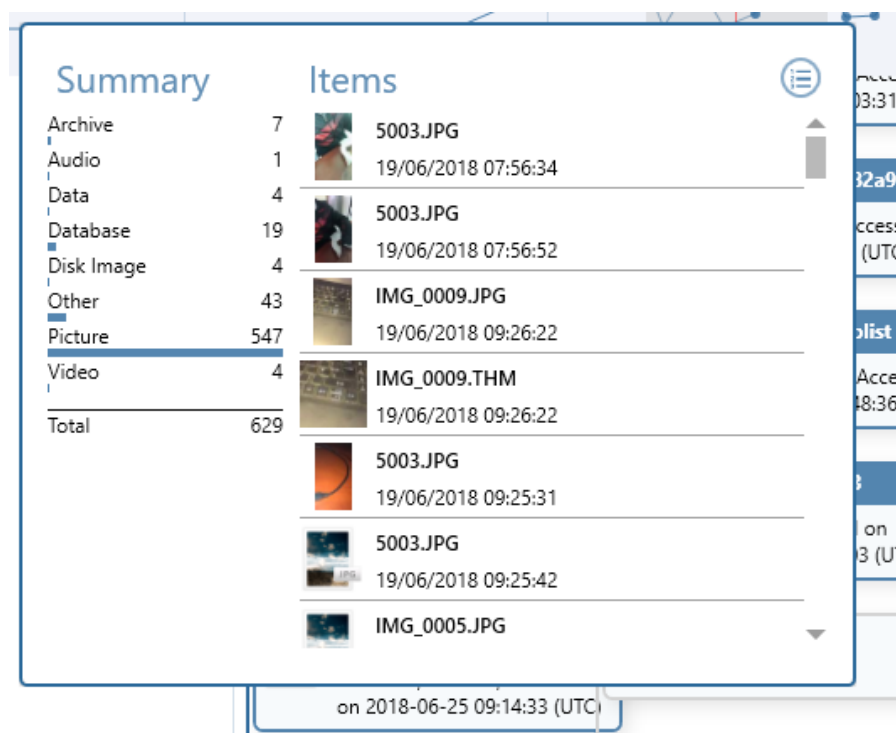


When the Timeline is limited in this way, you will also see a button next to the Scale control, as shown above, and a red warning message to indicate the view is a subset of the filtered data.

If this is clicked, the current view will be released from the restriction, and the view will be refreshed to show the next highest scale. This behaves, in a way, like a 'back' button. If this icon is present, it will be disabled when the current view is added as a snapshot. This is because the date restriction is now under the control of the snapshot. If you scroll the Timeline and the current snapshot (if any) is then deselected, this icon will be enabled again, thus indicating that the Timeline is still under time restrictions and that you can again remove that by clicking the icon.

GROUPED ITEM HOVER INFORMATION

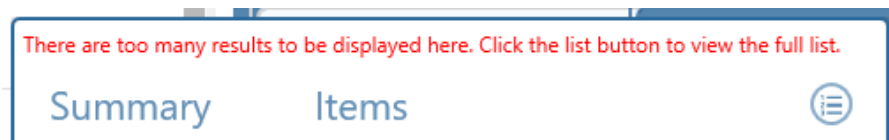
Figure 472



The window in the above image is shown when clicking the  icon in a grouped item. This gives a summary graph showing the types in the group, their count and size relative to the entire group (in the form of a bar). The items in the group will be shown in a list and can be selected using normal taggable item control methods. The thumbnail images are loaded as you scroll. The list view button in the top left can jump to the Analyse list view, showing only the items in this group. You can then use all the normal filters and sort amongst just those items from the filter. The restriction can be lifted when you reset the date filter.

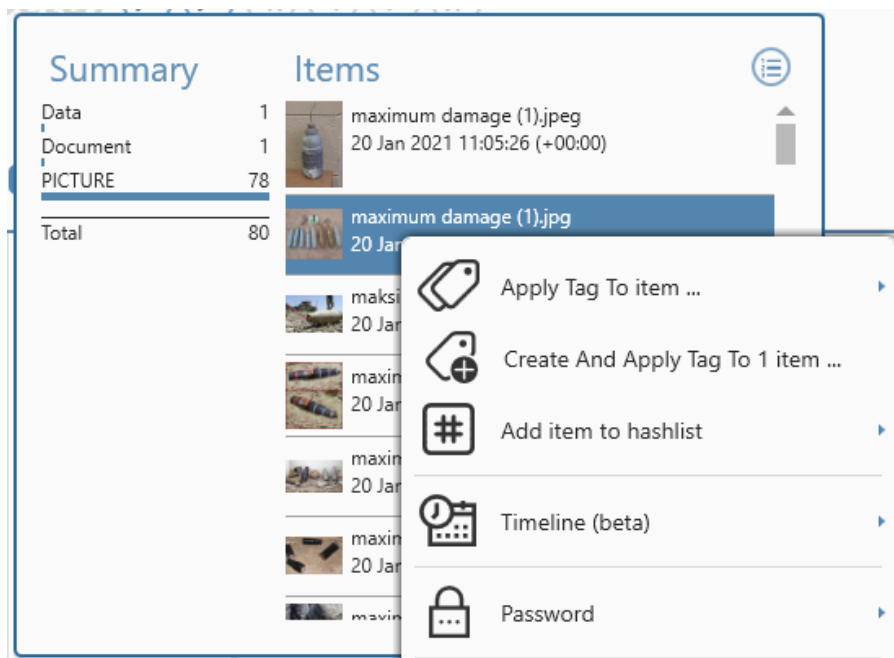
Note! If there are 1000 items or more in the group, you will see the below message.

Figure 473



Accessing the taggable context menu from this list is also possible by right-clicking an item.

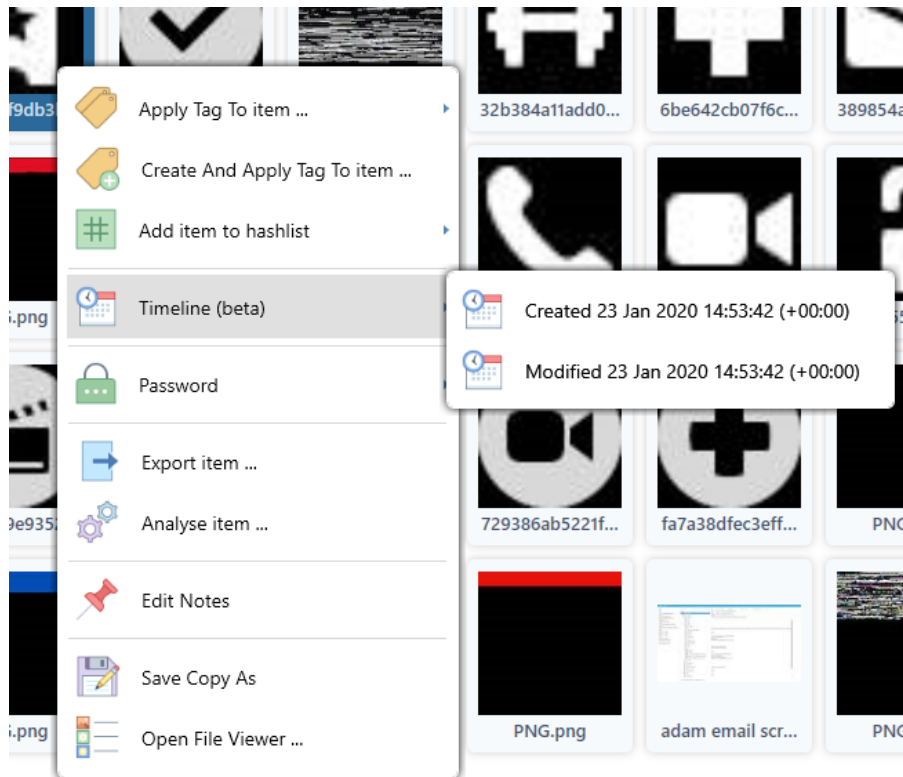
Figure 474



TIMELINE FROM OTHER VIEWS

In other Analyse views, using the Timeline option in the context menu to go to the Timeline view from a taggable item is possible. You can select one of the item's date properties, which will be the time position of the view when loaded.

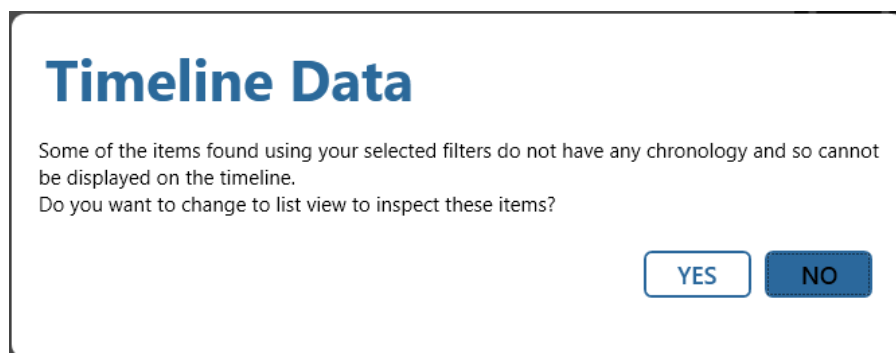
Figure 475



CHECKING FILTER RESULTS

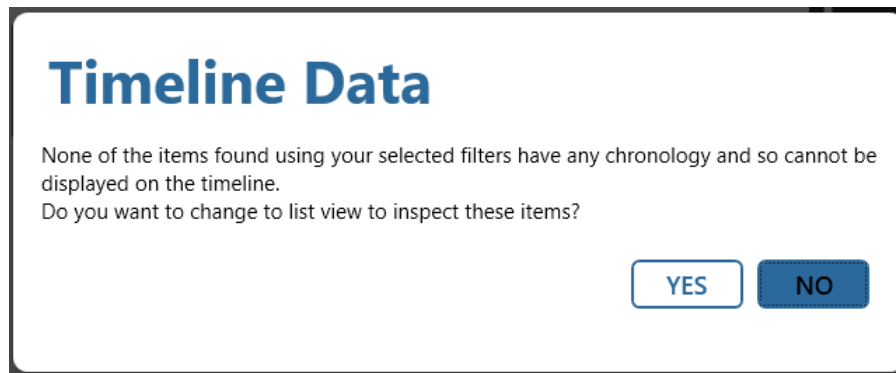
The Timeline query will only return items that have date properties. This is because they need to be placed on the Timeline in the correct location. The usual Analyse filters do not rely on date properties except when a date filter is added; therefore, there may be instances when the Timeline results do not contain all items expected by your choice of filters. In this case, the error below may be shown.

Figure 476



Some taggable types may not contain any date information (such as participants). In this case, the error message below will be shown.

Figure 477



If you use the Timeline above other views, such as the gallery, only the warning will be displayed, and it will not prompt you to switch views.

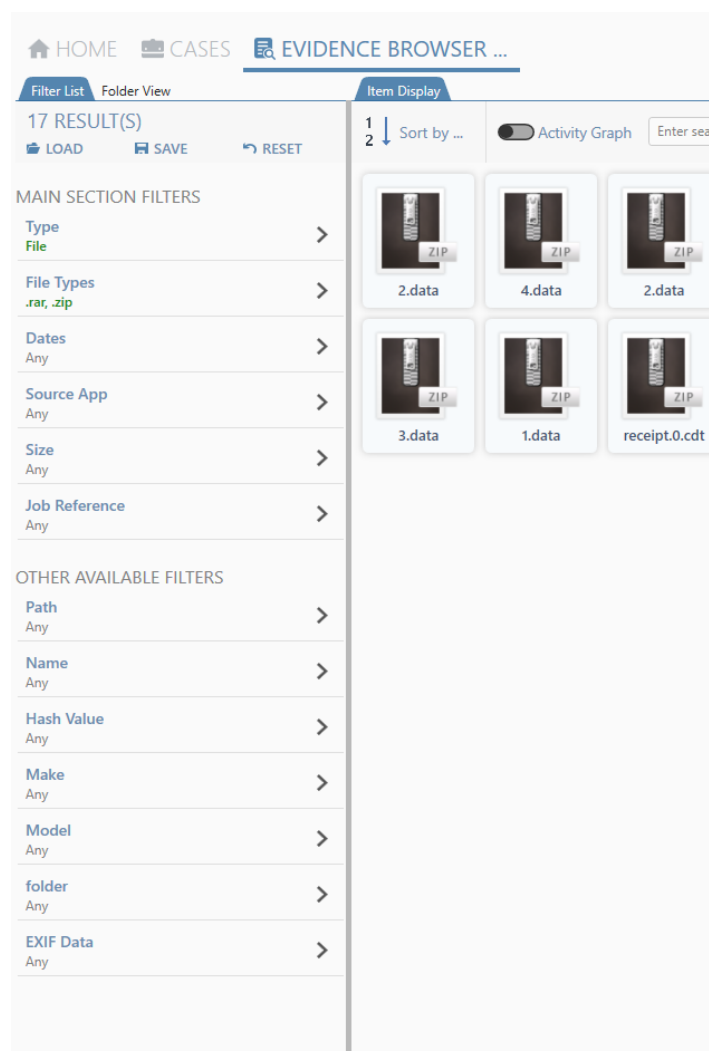
6.7. FILE FILTERING

File Filtering allows the investigator to filter through the masses of data that has been acquired.

To add a filter, follow these steps:

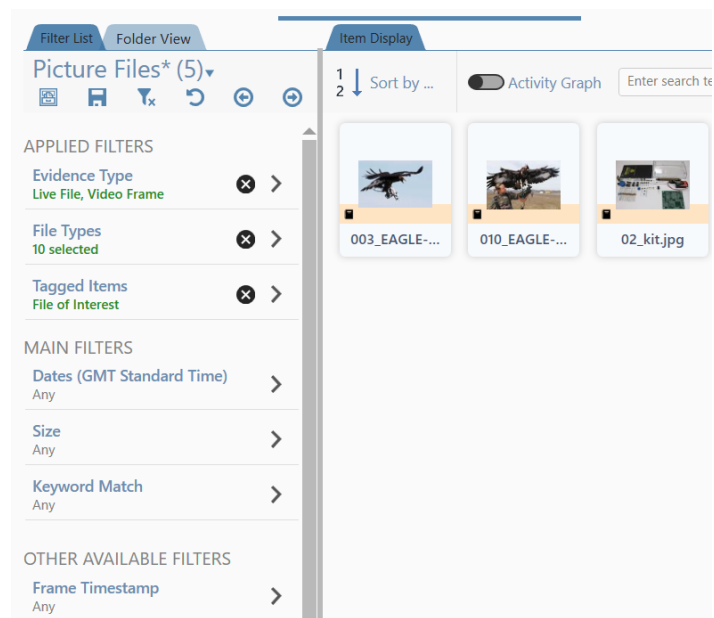
- From the Detego Analyse home screen, click the 'Analyse and Manage' tool tile.
- Select the case you want to view from the 'CASE LIST' column on the left side of the screen.
- Click the 'All files' tab from the 'Exhibit Content' tab.
- Add a new filter by selecting any filters down the left side panel.

Figure 478



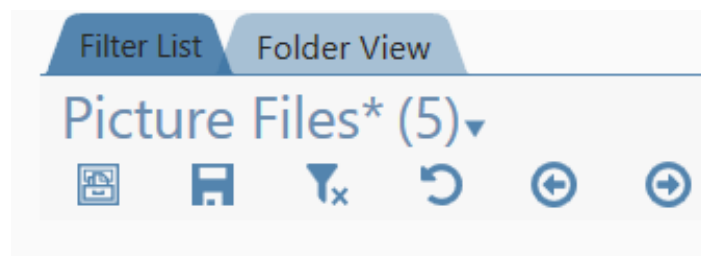
- Once an individual filter has been applied, move that filter to an **'Applied Filters'** section at the top of the list of filters, and each applied filter will have a "delete/remove" icon; once it is removed, it will add an entry to the filter stack, and it is removed from the "Applied Filters" section, will return to its normal place in the list of filters.

Figure 479



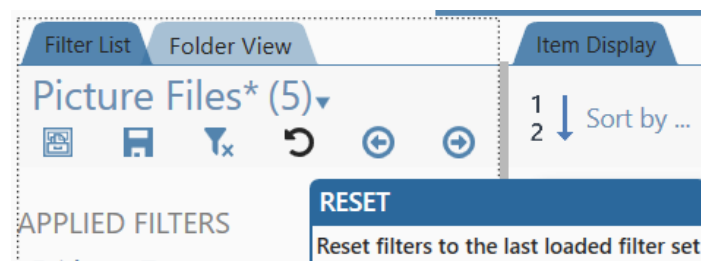
- **Back, Forward, and Remove All** buttons are newly added to the filter panel to allow users to move back/forward through the filter stack to a previous filter set and to remove all filters.

Figure 480



- Changed the existing "**Reset**" Icon to make it clearer that it is a reset icon and not an undo/back icon

Figure 481



- The text for the Manage, Save and Reset icons has been removed, and hover text has been added for each icon in the filter panel.

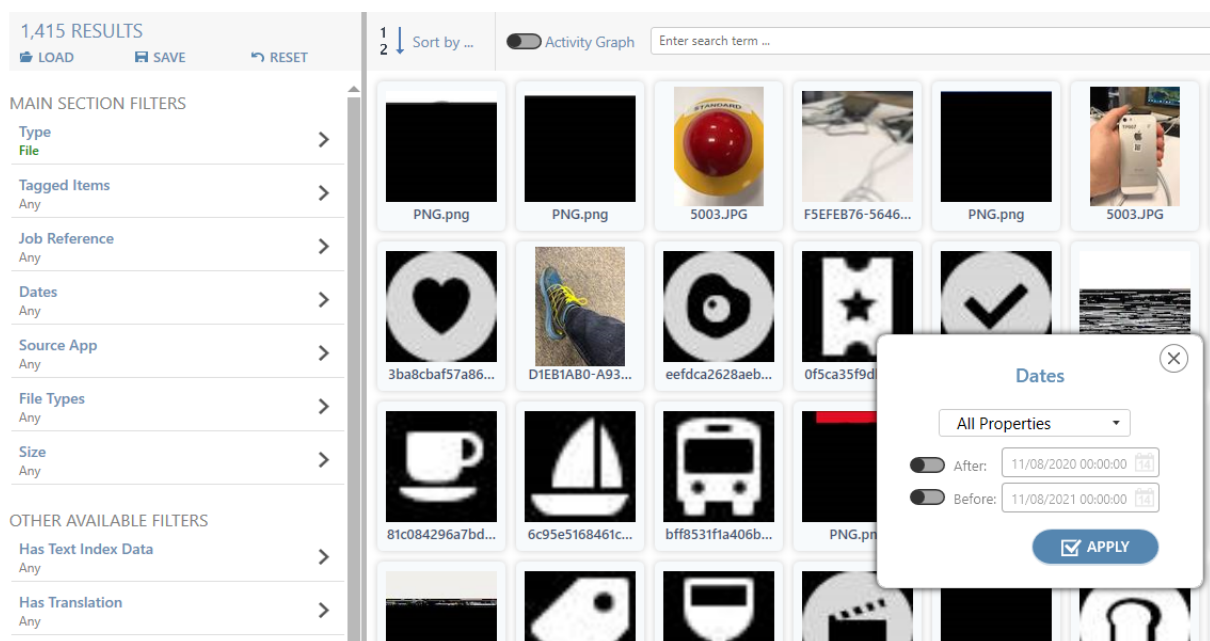
FILTERING BY TIMESTAMPS (ACCESSED, CREATED OR MODIFIED DATES)

To filter by timestamp, follow these steps:

- Select the 'Dates' filter in the Filter List panel on the left.
- Choose from the dropdown in the popup window 'Accessed', 'Modified' or 'Created'.
- Choose your period. This can be narrowed down by selecting both 'After' and 'Before' and choosing certain dates required.
- When you are happy with the Dates, click APPLY.
- If you want to remove the filter, click the 'Dates' filter again, remove your selection, and click APPLY.

NOTE! You can now filter files by deleted/carved tags.

Figure 482



FILTERING BY HASH VALUES (SHA1 & MD5)

To filter by hash values, follow these steps:

- Click the 'Hash' filter in the Filter List panel on the left.

- Select the underlined 'contains', creating a menu to select how you search for the hash value.

These include:

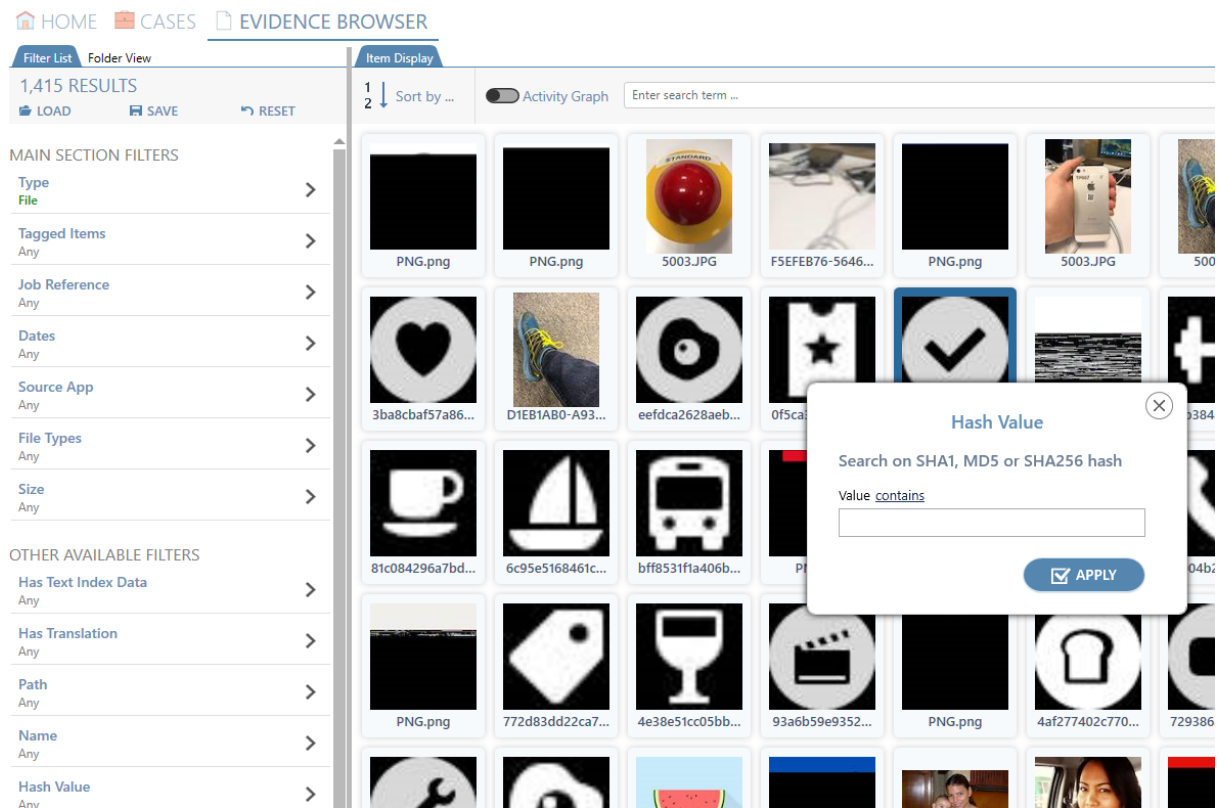
1. 'Contains'
2. 'Starts With'
3. 'Ends With'
4. 'Equals'
5. 'Regex'

'Does Not' opens up another menu giving the following options:

1. 'Contain'
2. 'Start With'
3. 'End With'
4. 'Equal'
5. 'Match'

- Type in the value.
- Click APPLY.
- To remove, click the 'Hash Value' filter, remove the value and select APPLY.

Figure 483

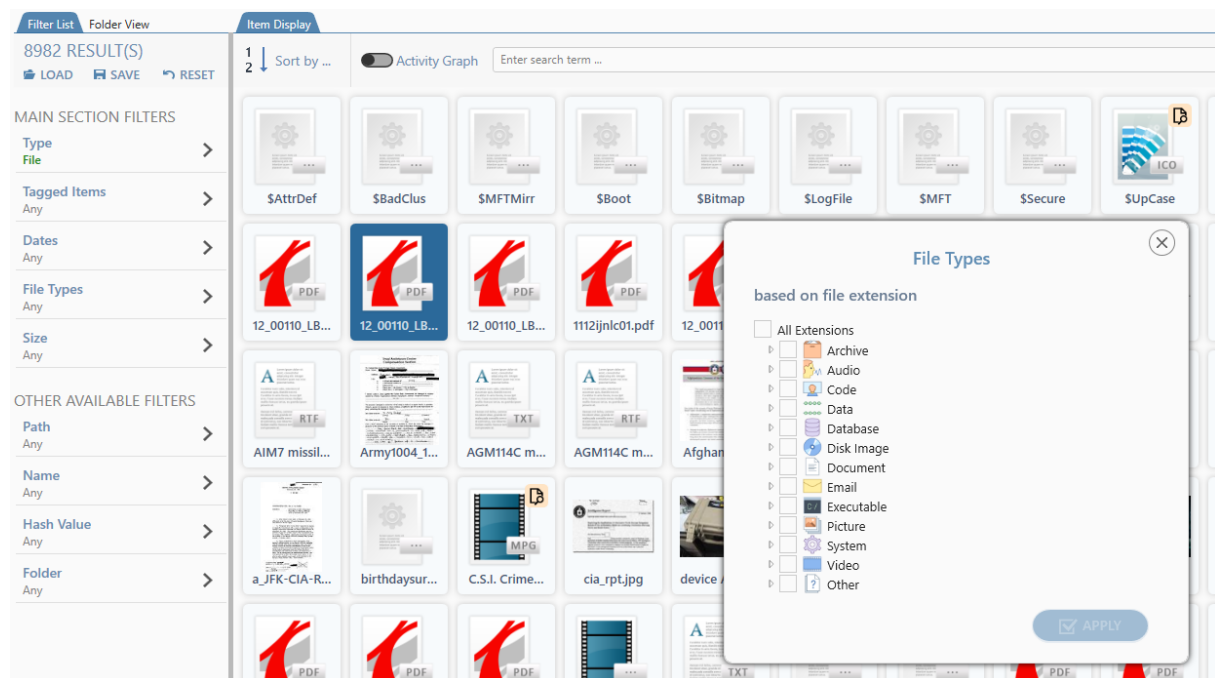


FILTER BY EXTENSION

To filter by extension, follow these steps:

- Select the 'Extension' filter on the left side panel in the Filter List.
- Select each checkbox you want to filter extensions or click the top-left checkbox that says 'All Extensions'.
- Once you are happy with your selection, click APPLY.
- If you want to remove the filter, click the 'Extension' filter, remove the selected checkboxes, and click APPLY.

Figure 484



SAVING FILTERS

Filter selections can be saved and used throughout your exhibit or all exhibits.

Figure 485

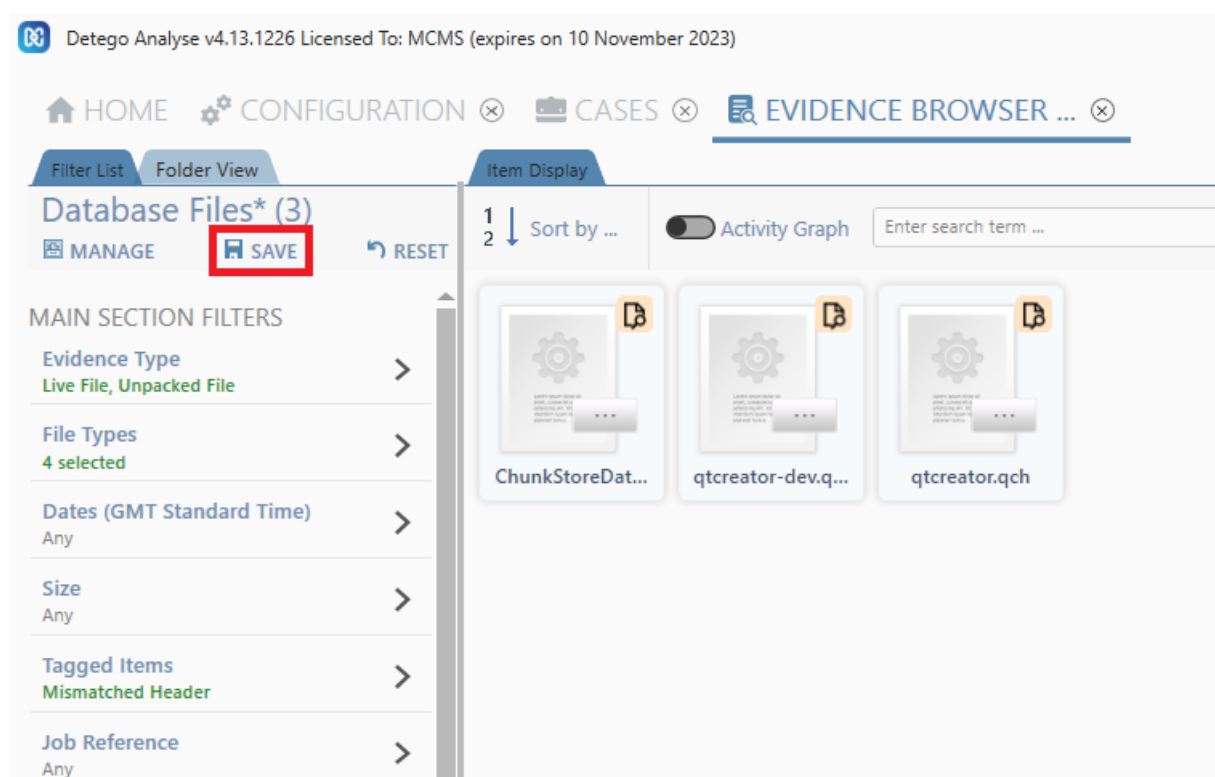
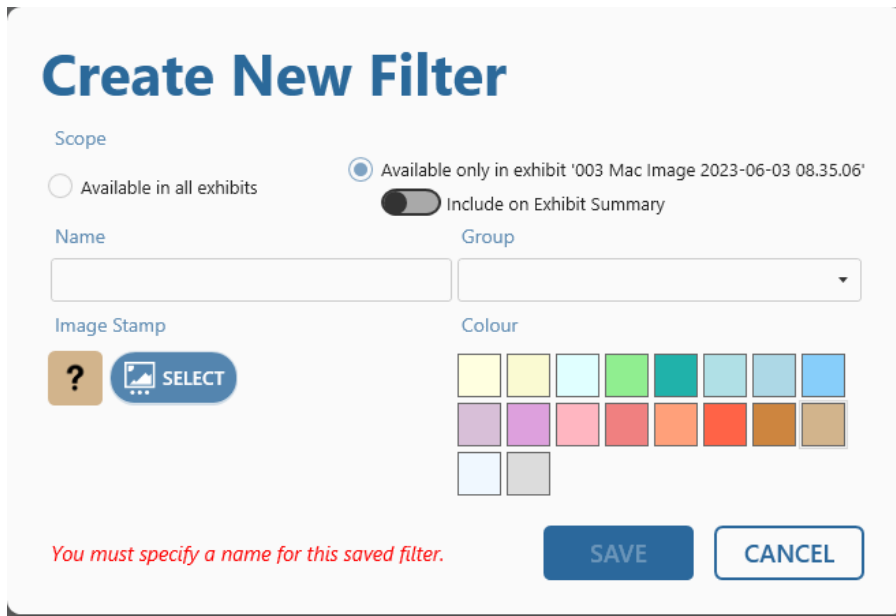


Figure 486



Create New Filter

Scope

☐ Available in all exhibits ☒ Available only in exhibit '003 Mac Image 2023-06-03 08.35.06'

☐ Include on Exhibit Summary

Name

Group

Image Stamp

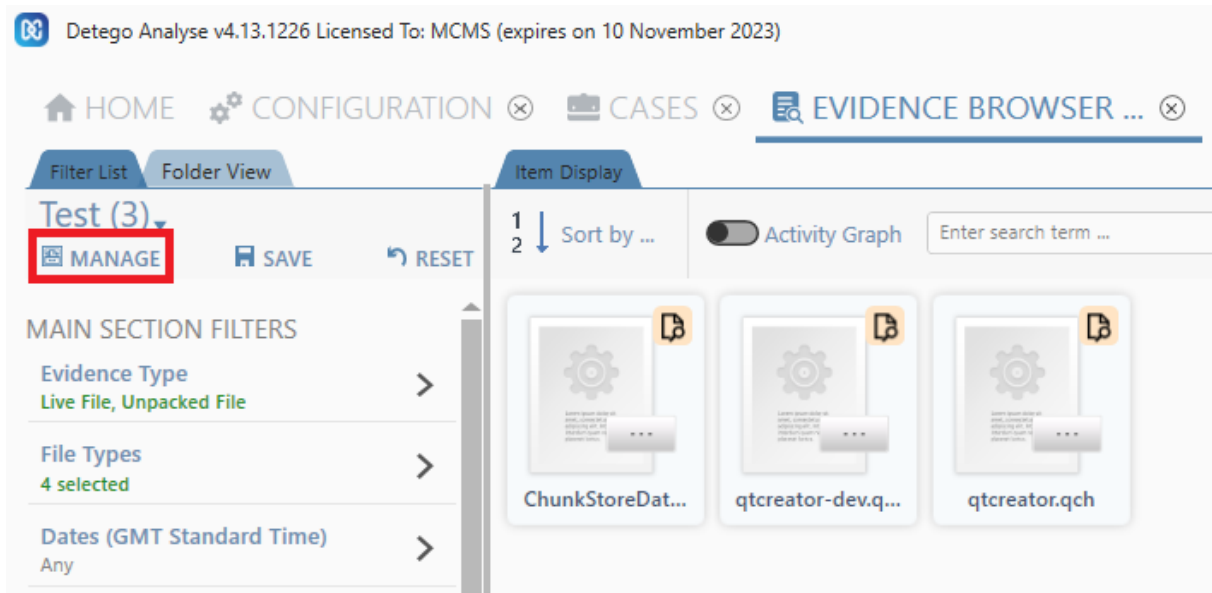
Colour

You must specify a name for this saved filter.

You can name the Filter selection and select a colour and image stamp to identify them easily.

You can click the 'Manage' button above the filters to change the filter from exhibit only to all exhibits or vice versa.

Figure 487



Detego Analyse v4.13.1226 Licensed To: MCMS (expires on 10 November 2023)

HOME CONFIGURATION CASES EVIDENCE BROWSER ...

Filter List Folder View Item Display

Test (3)

MAIN SECTION FILTERS

Evidence Type
Live File, Unpacked File

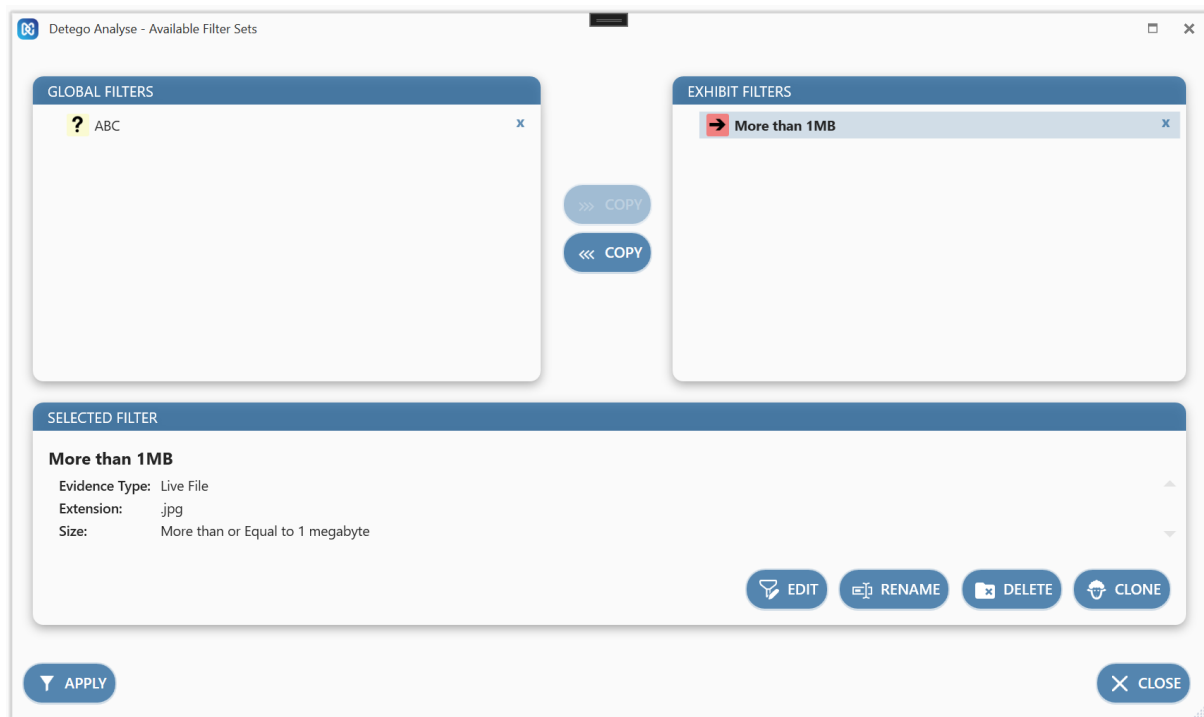
File Types
4 selected

Dates (GMT Standard Time)
Any

1 2 Sort by ... ☐ Activity Graph Enter search term ...

ChunkStoreDat... qtcreator-dev.q... qtcreator.qch

Figure 488



Once you select the filter you wish to change, you will be given options for the following:

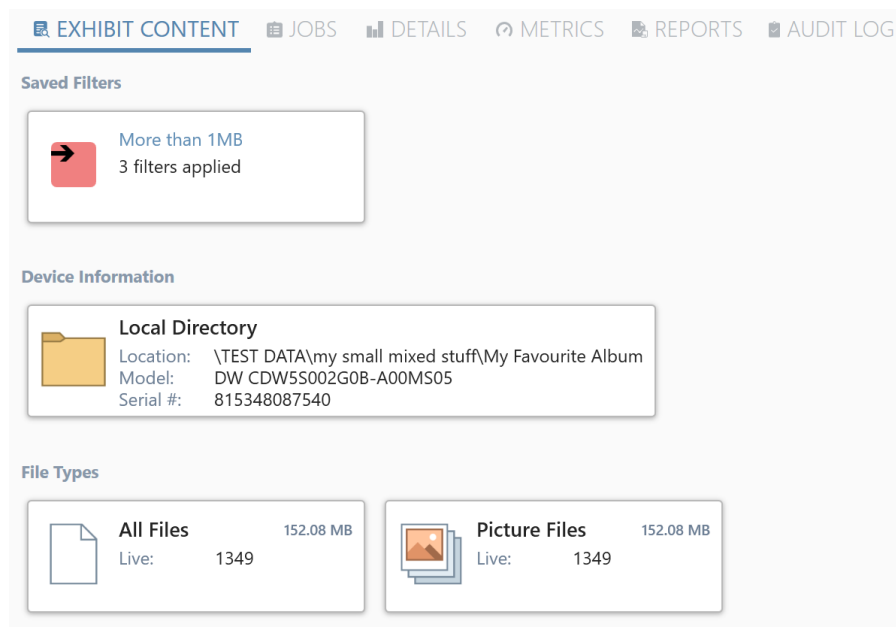
- **Copy** - Makes a copy from Global Filters to Exhibit Filters or vice versa.
- **Edit** - Edit the colour, name, symbol, group etc
- **Rename** - Change the filter's name
- **Delete** - Removed the filter
- **Clone** - Makes a copy of the filter, which will stay in the exhibit it originated from.

Saved filters are now persisted in the database rather than exclusively stored on the client.

Global filters are stored in the core database. In contrast, per-exhibit filters can be attached to a specific exhibit and will travel with that exhibit when exported or stored on a portable storage volume.

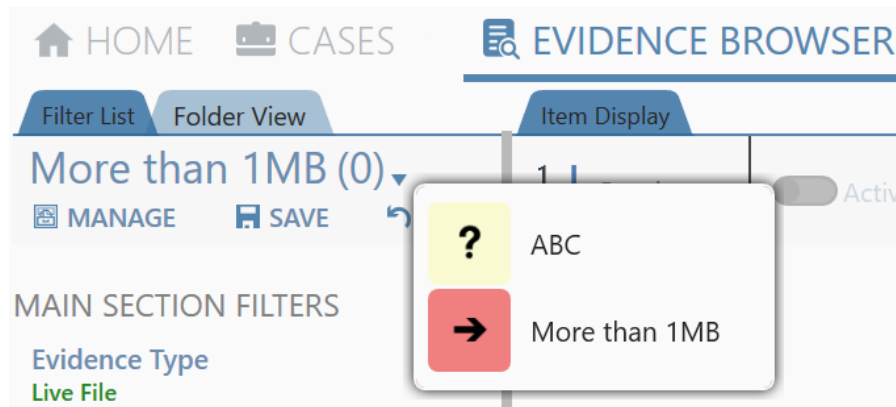
Per-exhibit filters can be set to appear on the exhibit contents view for the exhibit:

Figure 489



The filter header panel now includes a dropdown menu which can be used to apply saved filters quickly:

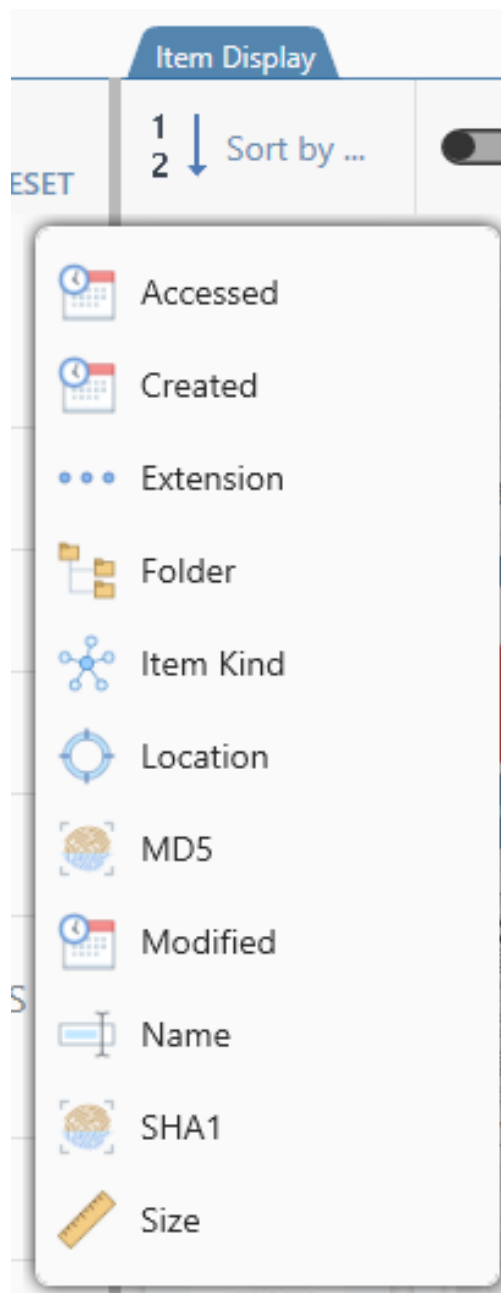
Figure 490



6.8. FILE SORTING

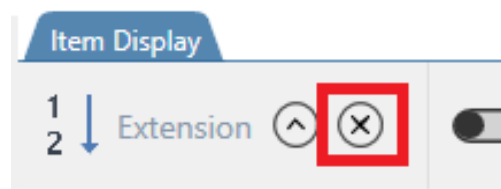
Sorting enables you to arrange files according to your preferred parameters, accessed by clicking the 'Sort by...' icon in the top left corner of the 'Item Display' tab.

Figure 491



Selecting another sort parameter replaces the previous parameter. Clear the parameter by clicking the 'X' icon next to it.

Figure 492



USING TAGS

Tags (also called bookmarks) allow the operator to group files of interest for their case. The investigator can create their list of tags via the Configuration module and use the predefined Tags supplied.

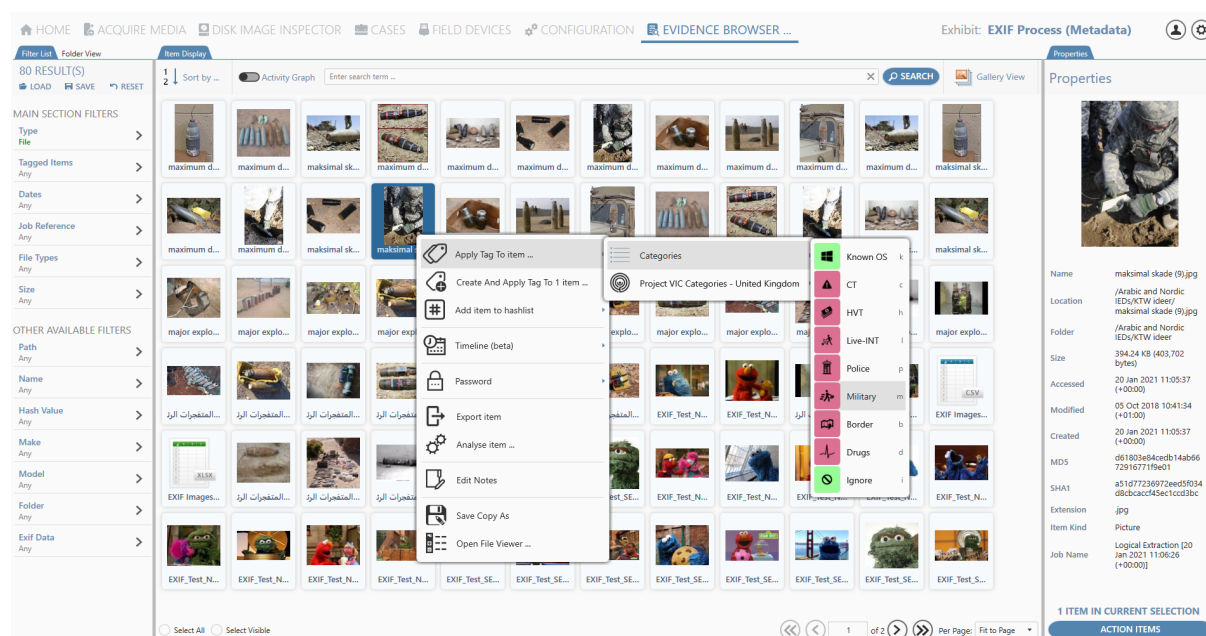
Files can either be tagged manually by the investigator or automatically tagged when running an analytic such as a Hash or Keyword list across a dataset.

To add a tag manually, follow these steps:

- In the Evidence Browser, locate the file(s) you wish to tag (hold down the shift button to select multiple files) and either enter the specific shortcut key for the tagging type or right-click and select 'Apply Tag' and then 'Categories' to view all the available tags.
- Select the tag you want to assign to the file(s). The tag's colour, title, and icon will be applied to the field(s).

Note: The operator configured Red tags as unsafe and green tags as safe.

Figure 493



CREATING AND APPLYING TAGS

The operator can also create and apply tags from the Evidence Browser. The new tag will be added to the Tags list in the Configuration module (refer to Configuring Tags).

To add and apply a tag, follow these steps:

- In the Evidence Browser, locate the file(s) you wish to tag (hold down the shift button to select multiple files and right-click. From the drop-down, select 'Create and Apply Tag'.
- Enter a name in the pop-up that appears and then choose a tag group from the drop-down to house the new tag.
- Select an image stamp and a colour to identify the new tag.
- Create a keyboard shortcut by configuring the sliding buttons and drop-down fields.
- Beneath the 'Viewable Status' title, choose whether the item in that group is 'Safe' or 'Unsafe' to view. This will change the tag colour to red if unsafe or green if safe.
- Click the 'SAVE' button to store the new tag. This will automatically apply the tag to the file(s) the operator initially selected.

Figure 494

Create and Apply Tag

Name:

Group:

Image Stamp:  

Key Shortcut: ☒ CONTROL ☒ SHIFT

Viewable Status: ☐ Items tagged with this tag are considered **unsafe** for viewing by default
☐ Items tagged with this tag are considered **safe** for viewing by default

SAVE **CANCEL**

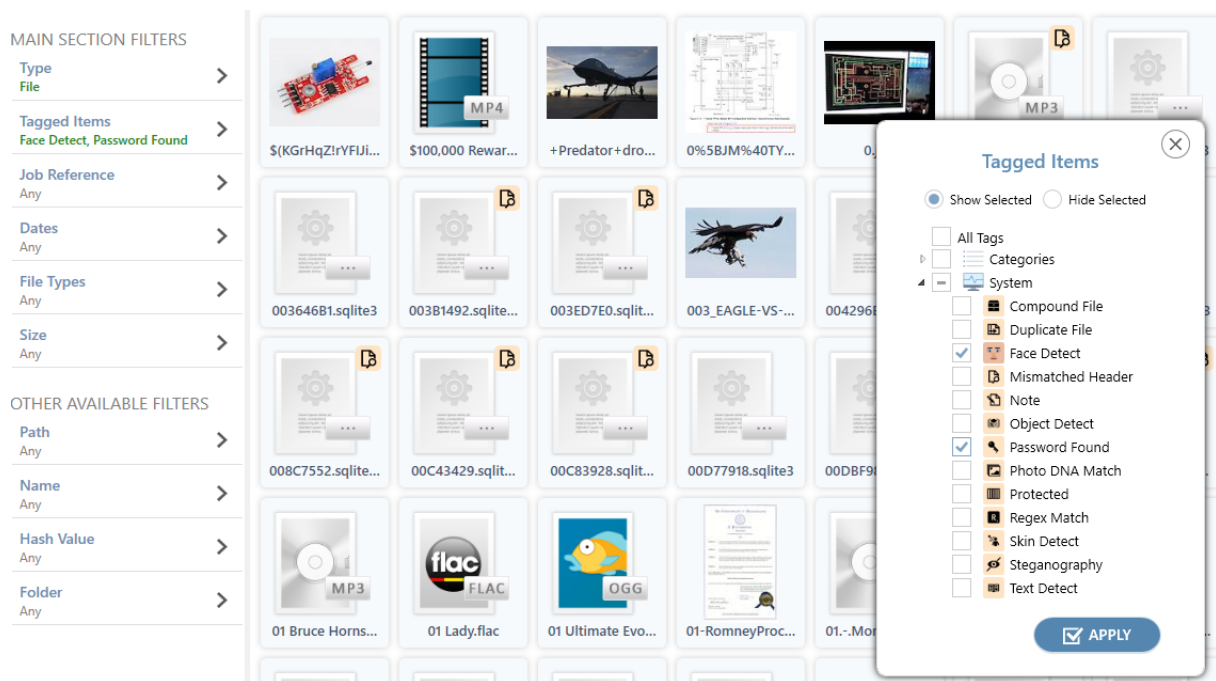
VIEW FILES PER TAG

Tagged files are identifiable by their unique pre-configured border colour and icon (refer to Configuring Tags). To filter files by tag, follow these steps:

- Click the 'Tagged Items' filter in the filter list on the left side panel.

- Select the tagged items you would like to display from the pop-up window.
- When you are happy with your selection, click APPLY.

Figure 495



CARVED FILES TAGS

This version of Detego extends support for files held in unallocated space. Files are now classified with a Deleted/Recovery Source property, which indicates whether they are live, carved from a live partition, or carved from unallocated space. Such files are now termed 'Deleted/Recovered Files'. Recovery typically involves an extra effort to reconstruct a file from one or more raw data sources.

Note that for recovered and deleted files, the deleted filter has been replaced by the 'Deleted/Recovery Source' filter; please use this new filter to identify recovered or deleted files as required. To exclude all deleted/recovered files when filtering in the evidence browser, please de-select 'Deleted/Recovered Files' in the 'Evidence Type' filter panel.

The sources for files that have been recovered are as follows:

- **Carved File System Unallocated** - a file recovered from unallocated portions of a known file system; these are typically considered deleted files

- **Carved File System Allocated** - a file recovered from allocated portions of a known file system; these are typically considered active/live files
- **Carved Partition Raw** - a file recovered from a partition that has an unknown structure; these could be active/live or deleted files
- **Carved Disk Raw** - a file recovered from a raw disk that has an unknown structure; these could be active/live or deleted files
- **Windows Recycle Bin** - a file recovered from the Windows Recycle Bin, metadata such as file name is also recovered; these are typically considered as deleted files
- **macOS Trash** - a file recovered from the macOS Trash, metadata such as file name is also recovered; these are typically considered deleted files

On the Evidence Browser view, files with a 'carved' recovery source will appear with a 'knife' icon overlaid, and files recovered that are considered deleted will appear with a 'trashcan' icon overlaid. Note that it's possible to have both the carved and deleted icons on a single item.

Figure 496

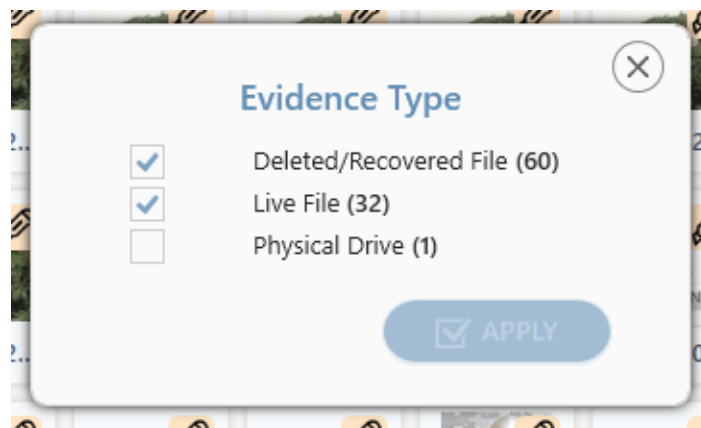


Figure 497

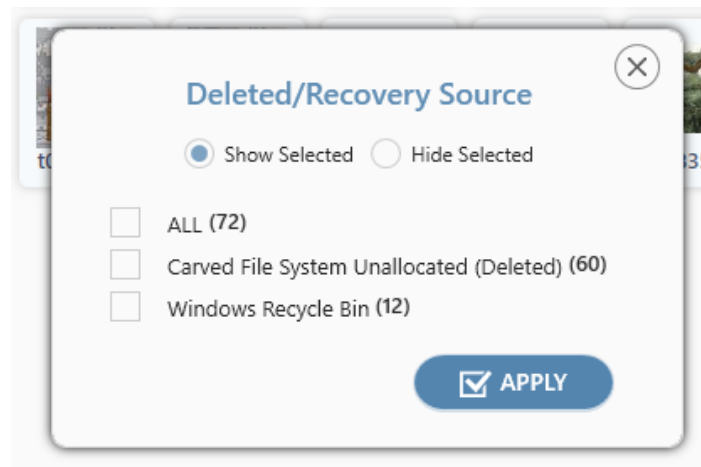
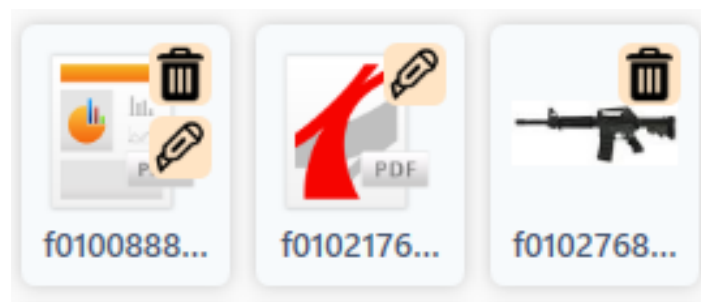


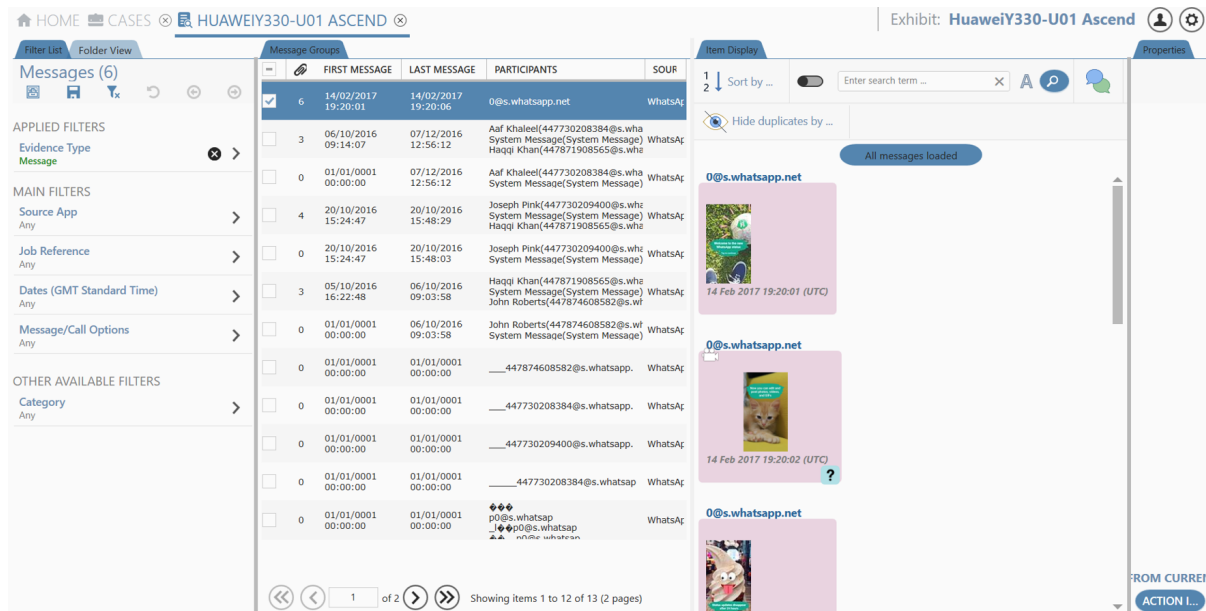
Figure 498



MESSAGE VIEW

Message Display provides the ability to browse through a set of message groups/threads and see high level details, allowing you to drill down to the individual messages within a thread.

Figure 499



- The left panel is your filter panel.
- The centre panel displays the Message Groups and includes the following details:
 - Number of Attachments within the thread
 - First Message Timestamp
 - Last Message Timestamp
 - Participants
 - Source
- The right panel will display the selected group/thread.

NOTE! If you are viewing messages on an exhibit that was imported on a version of Detego Analyse before 4.16 then you the data will still be grouped as it was previously. To use the new layout, you must re-import the original extraction.

6.9. THE PORTABLE VIEWER

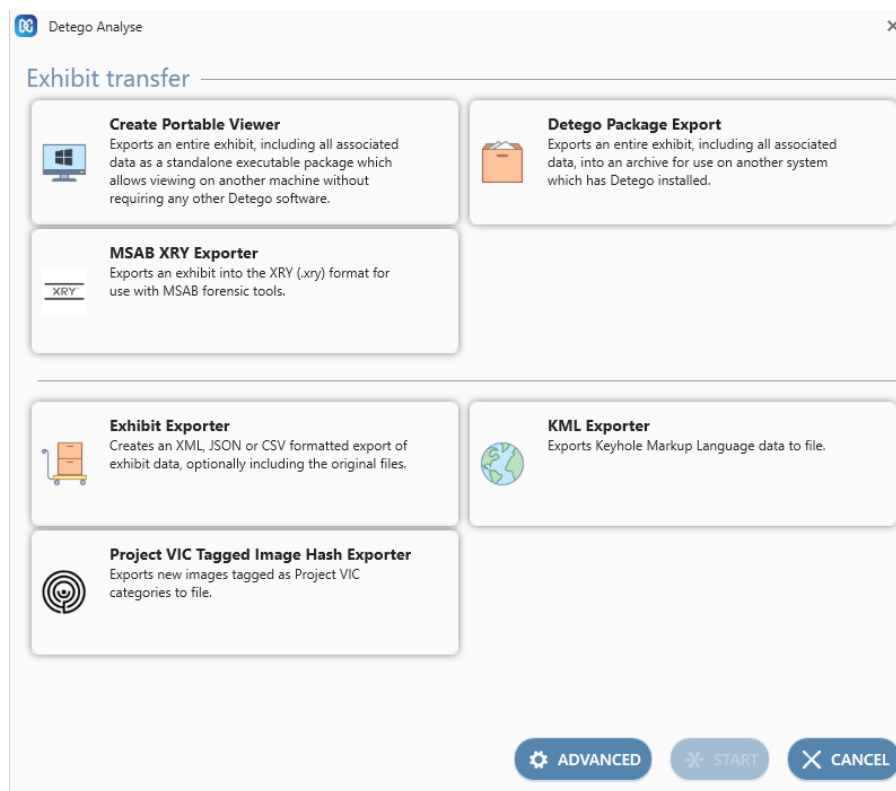
The Portable Viewer is a portable investigation viewer. It exports an entire exhibit, including all binary artefacts and database entries, as a standalone executable package, allowing viewing on another machine. This is particularly useful for users who must give their findings to a reviewer.

EXPORTING TO PORTABLE VIEWER

To export an exhibit as a Portable Viewer package, please follow the below steps:

- Select an exhibit you wish to export from the Case List and select the 'Export' button in the bottom right corner.
- Under 'Exhibit Transfer', select the 'Create Portable Viewer' tile on the Export window.

Figure 500



- Firstly, type in the file path in the 'Create In' box OR select the button on the right and navigate to where you want to save the package.

Figure 501

Detego Analyse

Create Portable Viewer

Create In : Please select a folder in which to create the Portable Viewer tool

Reviewer : Please enter the reviewer's name here Password : Enter password here

☒ Include Reports in Portable Viewer

☒ Include Audit Trail in Portable Viewer

☒ Include Warning Message that Examination may contain restricted content-

Options :

☒ Include Portable Viewer program with output file

Required for first export to any reviewer. Turn off to improve export time.

Please enter any notes for the reviewer here

Notes :

• Output folder missing

• Restricted content description missing

• Reviewer name missing

• Password missing

DONE CANCEL

- Once you have selected where to save the package export, type in the Reviewer's name (person designated for) and a password you wish to use if you would like to password-protect the portable viewer exhibit.

Please Note! A password is required if the "Restricted Content" toggle is switched on.

Figure 502

Detego Analyse

Create Portable Viewer

Create In : Please select a folder in which to create the Portable Viewer tool

Reviewer : Please enter the reviewer's name here Password : Enter password here

Options :

- ☒ Include Reports in Portable Viewer
- ☒ Include Audit Trail in Portable Viewer
- ☒ Include Warning Message that Examination may contain restricted content-
- ☒ Include Portable Viewer program with output file
Required for first export to any reviewer. Turn off to improve export time.

Notes : Please enter any notes for the reviewer here

• Output folder missing
• Restricted content description missing
• Reviewer name missing
• Password missing

DONE CANCEL

- Select if you want any toggle button Options on or off (by default, they will all be switched on). See the details below for what each option does:
 - **Include Reports in Portable Viewer** – Allows the ability to see reports in the Portable Viewer
 - **Include Audit Trail in Portable Viewer** – Allows the ability to see the audit trail in the Portable Viewer
 - **Include a Warning Message that Examination may contain restricted content** – This allows you to select if the exhibit contains restricted content and, if so, include a warning message for examiners.
 - **Include the Portable Viewer program with the output file** – The Portable Viewer Installer will be exported along with the exhibit. This is required for the first export to any reviewer, but we recommend leaving it on in most cases.
- If you have switched on the Restricted Content toggle, you must select from the dropdown or type in a warning message for your examiners.

Figure 503

Detego Analyse

Create Portable Viewer

Create In: Please select a folder in which to create the Portable Viewer tool

Reviewer: Please enter the reviewer's name here Password: Enter password here

☒ Include Reports in Portable Viewer

☒ Include Audit Trail in Portable Viewer

☒ Include Warning Message that Examination may contain restricted content-

Options: RESTRICTED

Required for first export to any reviewer. Turn off to improve export time.

Please enter any notes for the reviewer here

Notes:

• Output folder missing

• Restricted content description missing

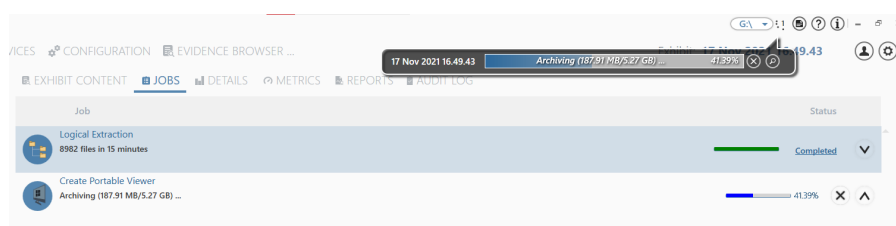
• Reviewer name missing

• Password missing

DONE CANCEL

- Insert any notes for the Reviewer in the 'Notes' section and then select Done.
- Once started, you'll be taken to the JOBS tab, and the progress bar will display above like other jobs. See below.

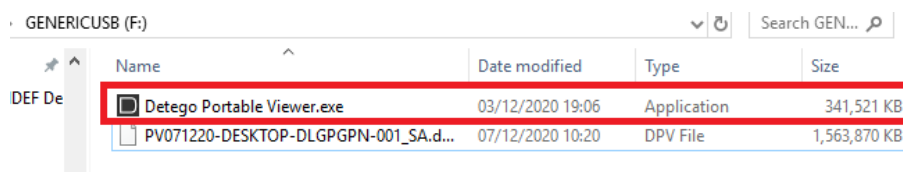
Figure 504



RUNNING DETEGO PORTABLE VIEWER

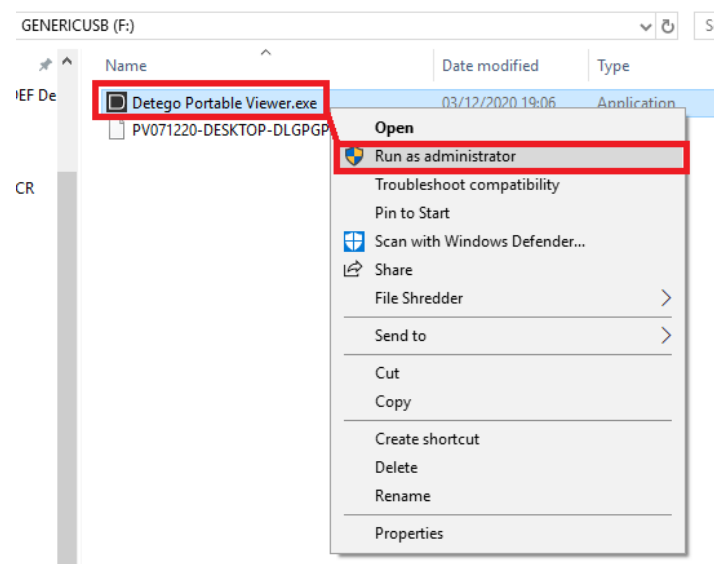
- Open the folder on the machine you wish to view the exhibit on. If it is a machine with Detego Portable Viewer installed or Detego Analyse installed, you shouldn't need to run the installer. If not, you should see the below or similar:

Figure 505



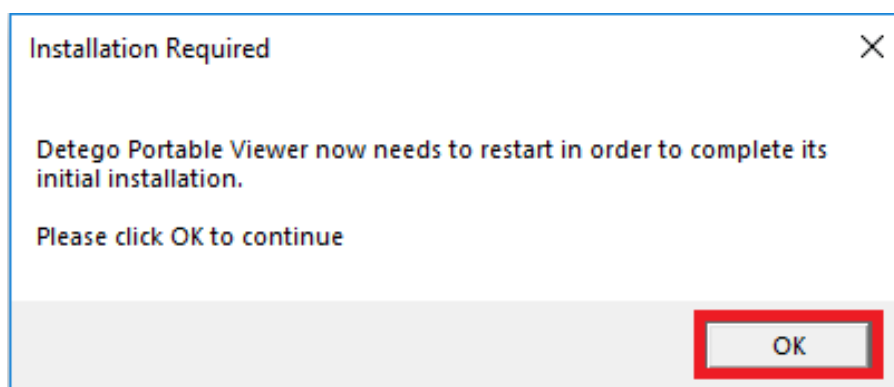
- You must run the 'Detego Portable Viewer.exe' to install the dependencies. Double-click or right-click and 'Run as administrator'.

Figure 506



- This will install the dependencies required to run Portable Viewer. Once this has finished, you will receive an Installation message, select OK to complete.

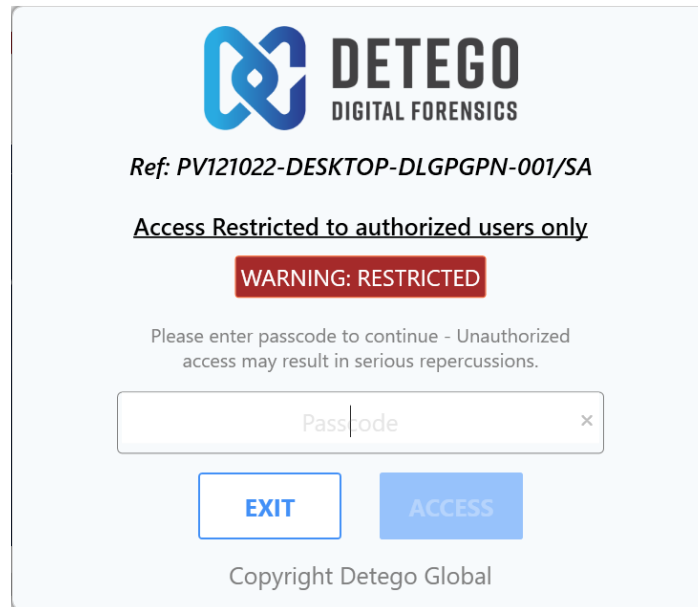
Figure 507



- A Windows UAC box will appear; select Open to continue.

- The Detego Portable Viewer will start, and you will (if selected when creating the export) be greeted by the Warning message. Input the Passcode you set or were given, and then select ACCESS.

Figure 508



- Wait for the Portable Viewer to load; depending on the computer's specifications, exhibit size, and background running tasks, this can take some time.

Figure 509



- If already installed on the machine, you can open the 'PV.... dpv' file, and it will run the export without installing the dependencies first.

Figure 510

Documents > Save Here > PortV			
Name	Date modified	Type	Size
Detego Portable Viewer.exe	03/12/2020 19:06	Application	341,521 KB
PV071220-DESKTOP-DLGP GPN-002_SA.dpv	07/12/2020 10:26	Detego Portable V...	1,563,871 KB

Detego Portable Viewer visualises as a more simplified Detego Analyse instance. The quick tabs at the top are determined by what you selected when creating the portable viewer export.

These can include:

- Exhibit Overview
- Audit Log
- Reports
- Exhibit Contents

Figure 511

Detego Portable Viewer v4.11.956

EXHIBIT CONTENT | REPORTS | AUDIT LOG

Device Information

Physical Drive
Model: JetFlash Transc...
Serial: 184WC63QWG...

File Types

All Files 8,962 total	Archive Files 713 total	Audio Files 106 total	Code Files 143 total	Data Files 380 total
Database Files 103 total	Disk Image Files 4 total	Document Files 824 total	Email Files 5 total	Executable Files 6 total
Picture Files 5,615 total	System Files 21 total	Video Files 229 total	Other Files 833 total	

Metadata (Right Sidebar):

Reference	17 Nov 2021 16:49:43
Initial Analyst	System Administrator
Exported On	12 Oct 2022 11:05:27 (+01:00)
Case Reference	Media Acquisitions
Exhibit Reference	17 Nov 2021 16:49:43
Reviewer	Test

Analyst Notes

Export Tags generated within Portable Viewer for importation to original exhibit

Export

CREATING TAGS FOR PORTABLE VIEWER

Follow these steps to create tags for portable view:

- Right-click an item in the Exhibit Content tab to create a tag and select 'Create and Apply Tag To item...'

Figure 512



- Fill in the details in the window and click SAVE; see the Creating Tags in Detego Analyse for more details.

Figure 513

Create and Apply Tag

Name

Group (no group)

Image Stamp ? SELECT

Key Shortcut CONTROL SHIFT

Viewable Status Items tagged with this tag are considered unsafe for viewing by default Items tagged with this tag are considered safe for viewing by default

You must specify a name for this tag.

SAVE CANCEL

APPLYING TAGS TO ITEMS IN PORTABLE VIEWER

To apply a tag to an item in Portable Viewer, right-click the item you wish to apply a tag to select 'Apply Tag To Item...' and then select a category or tag.

Figure 514

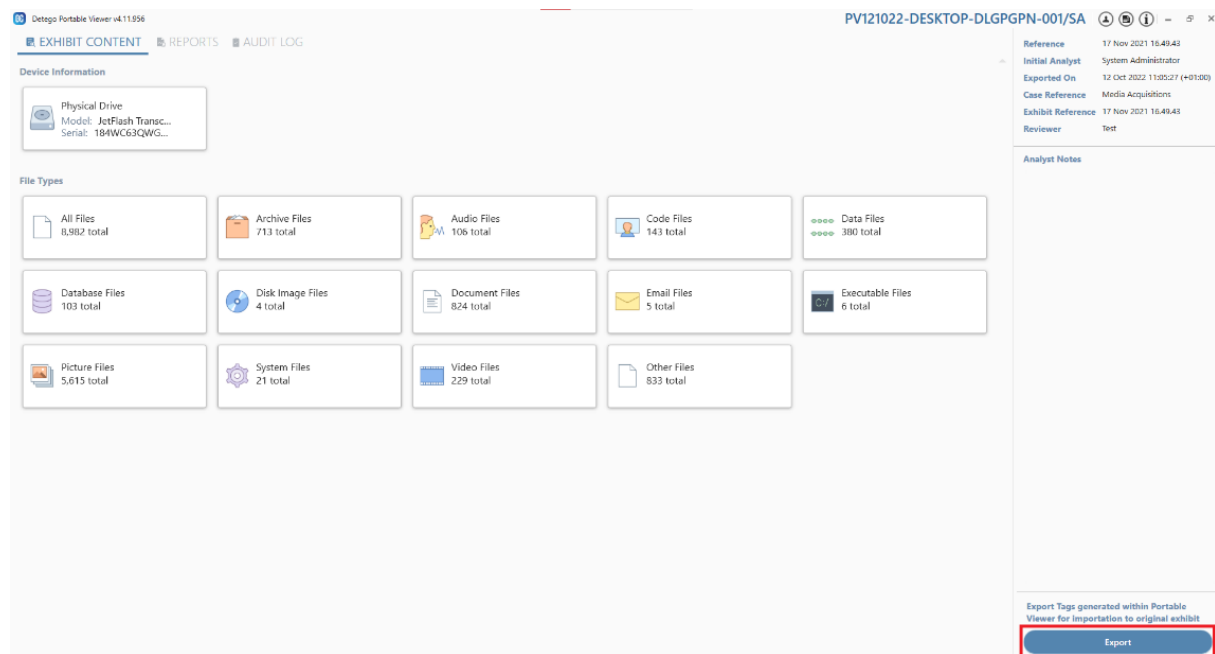


EXPORTING CREATED TAGS FROM PORTABLE VIEWER

To export created tags from Portable Viewer:

- Select Exhibit Overview and the 'EXPORT' button in the bottom right corner.

Figure 515



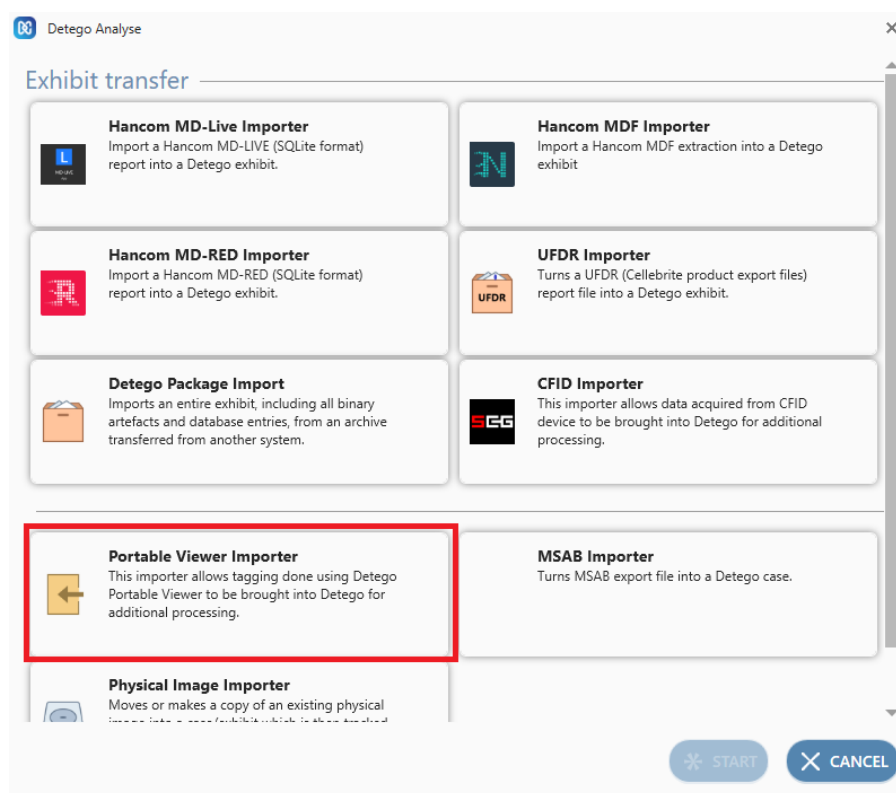
- Save the file to a folder and close Portable Viewer if you are done using it.

IMPORTING PORTABLE VIEWER

To import the tags added and created from Portable Viewer:

- Go to your Case List and select the exhibit you previously exported to a Portable Viewer.
- Click the IMPORT button and then select the Portable Viewer Importer tile.

Figure 516



- Once selected, the 'Portable Viewer Importer' window will open. Please select the file from wherever you saved it.

Figure 517

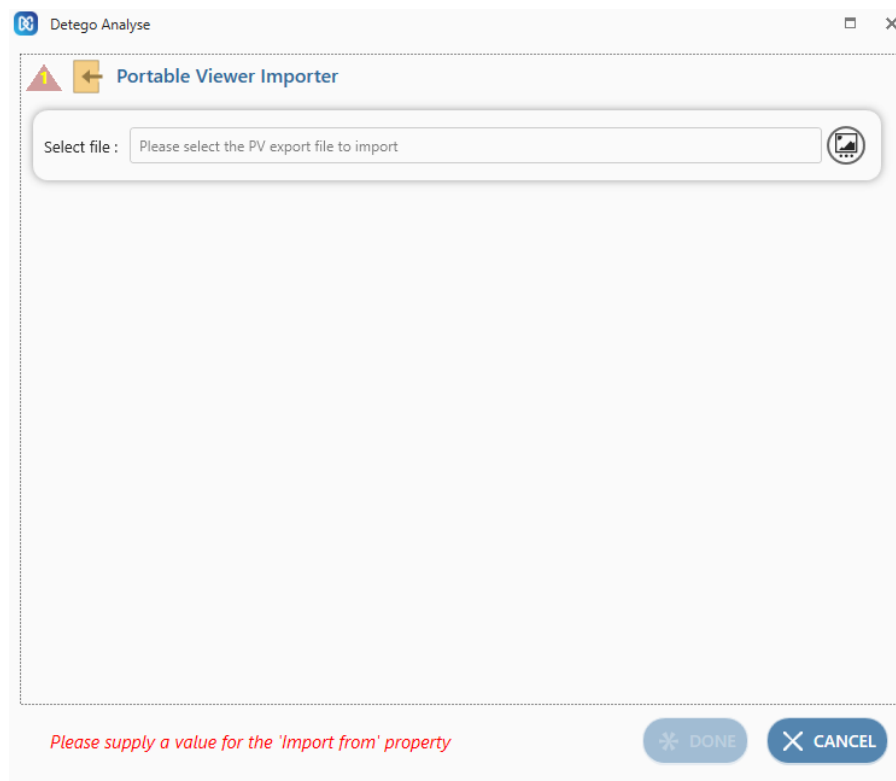
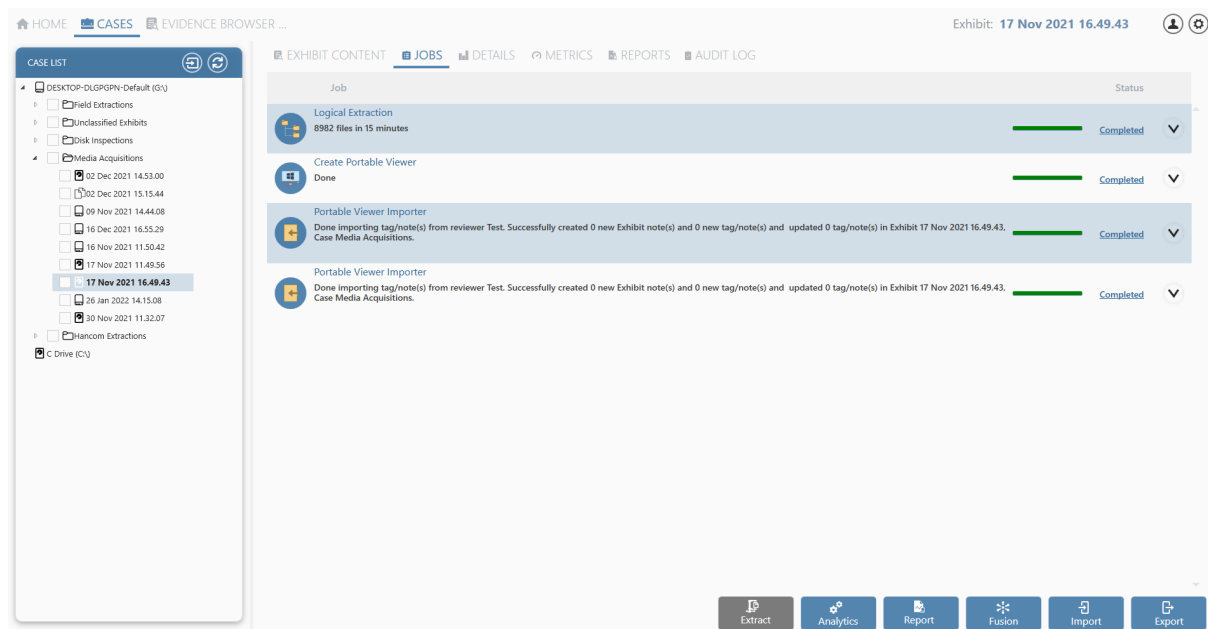


Figure 518



- Once you have imported successfully, the job will display as completed. If you click on the job, you can select the VIEW RESULTS button, which will take you to the 'Evidence Browser' and show you all tagged items imported from Portable Viewer.

Figure 519

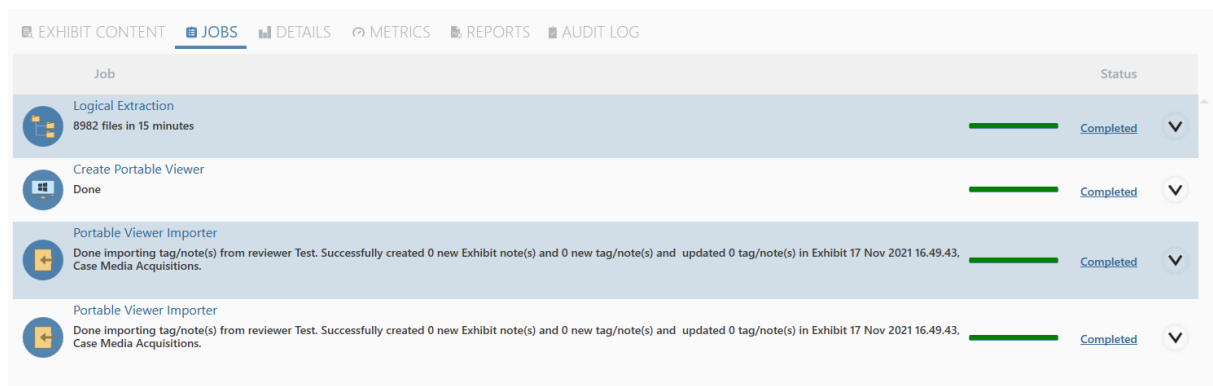
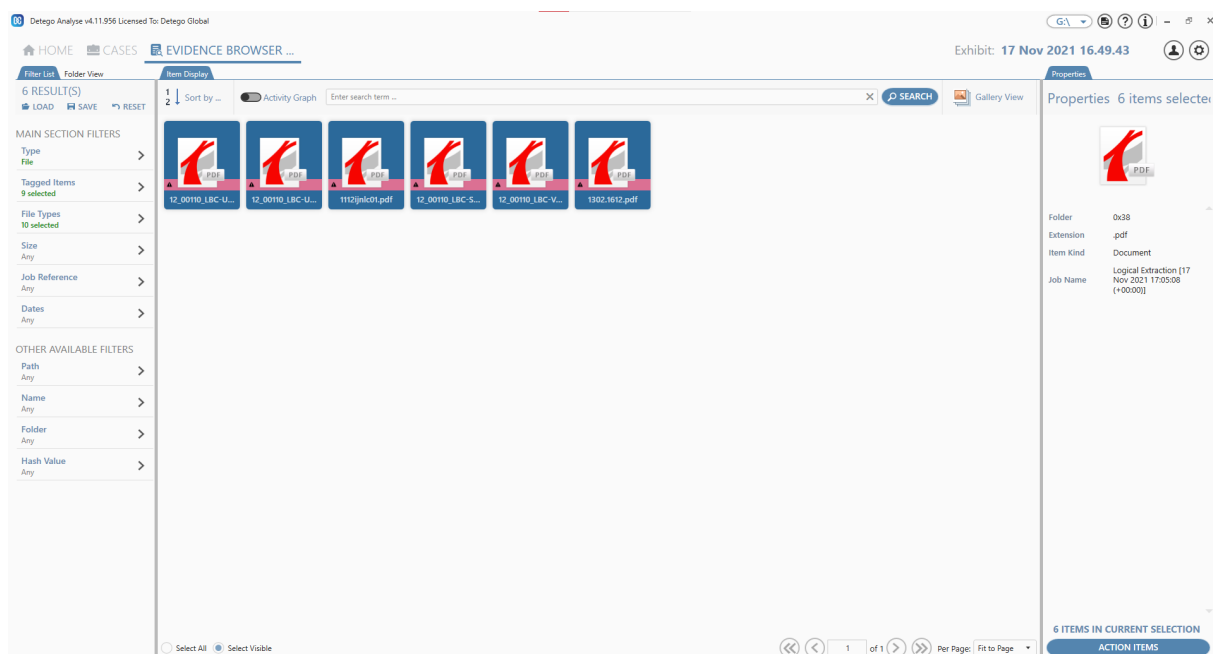


Figure 520



6.10. ANALYTICS

The Detego Unified Forensics Platform has a full suite of analytic options, helping the investigator analyse their exhibit rapidly. This allows them to dive deep into the data and identify the most pertinent intelligence to their case. Detego allows examiners to do more with less by harnessing advanced artificial intelligence and computing power.

Analysis options include acquiring usernames and passwords, detecting objects (weapons, drugs, vehicles, etc.), image indexing, EXIF data processing and much more. The operator can also automate these analytical options using various in-built and configurable forensic processing operations, leaving Detego to perform complex and manually intensive tasks.

SELECTIVE ANALYTICS

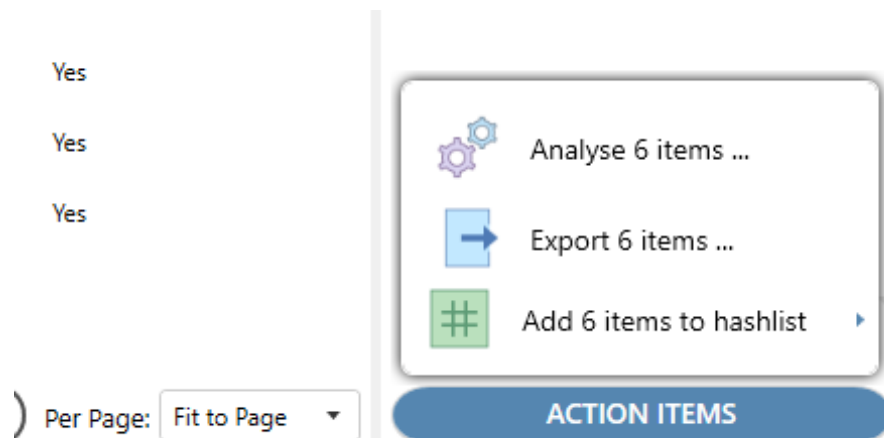
Where running analytics on all items within an exhibit is unnecessary, individuals or groups of selected artefacts can have analytics run only against them.

- From within the Evidence Browser – highlight or select the files you wish to analyse.
- Right-click any member of the selection and select 'Analyse X items.'
- Select the analytic(s) of choice and run.

Alternatively

- From within the Evidence Browser – highlight or select the files you wish to analyse.
- Click the 'X ITEMS IN CURRENT SELECTION' button in the lower right corner.
- Select 'Analytics'
- Select the analytic(s) of choice and run.

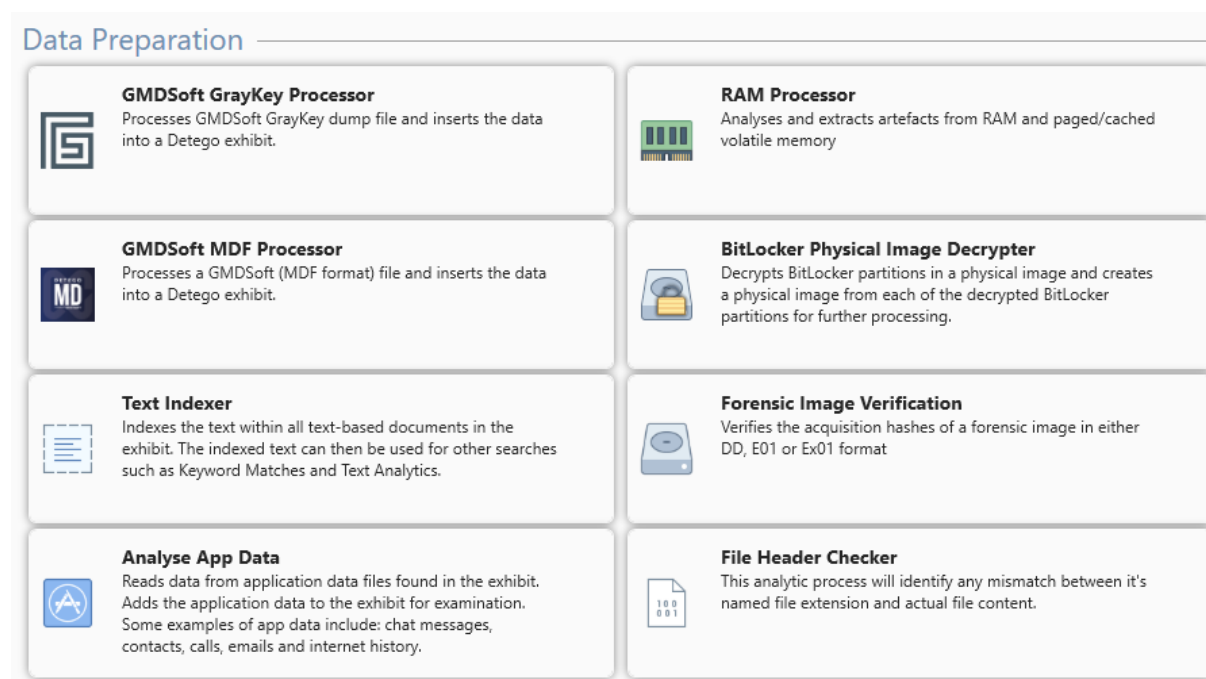
Figure 521



6.11. DATA PREPARATION ANALYTICS

The Data Preparation Analytical Process Section consists of jobs preparing the data for interpretation; some are required before running additional jobs.

Figure 522



GMDSOFT GRAYKEY PROCESSOR

Detego can import GrayKey dumps via the GMDSOFT software.

IMPORTANT NOTE! Detego MD must be installed and licensed correctly on the machine to process these GrayKey dumps. You will need to import a GrayKey dump prior to running the Processor job.

How To Run the Job:

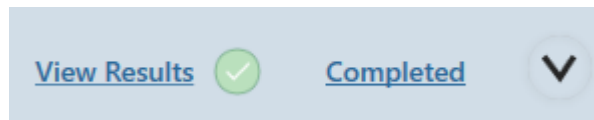
- Select the 'GMDSOFT GrayKey Processor' in the Analytics pop-up window, then select the START button to run the job.

Figure 523



- Once completed, you should see a lot of extra data extracted from the RAM Image in the EXHIBIT CONTENT tab; alternatively, you can select VIEW RESULTS to go straight to EVIDENCE BROWSER with all the files pulled from the job.

Figure 524



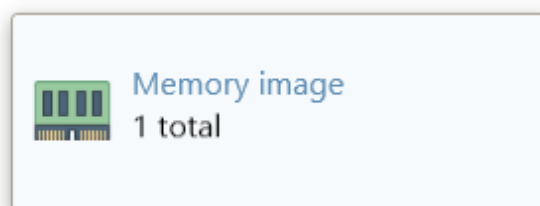
RAM PROCESSOR

The RAM Processor analyses and extracts RAM and paged/cached volatile memory artefacts. Therefore, this is a preconfigured job and cannot be altered in the 'ADVANCED...' customisation window.

Files that can be extracted from a RAM image include but are not limited to Cryptocurrency addresses, IP addresses, Social Media logins, Bank Cards, Application Data, Phone numbers and Email addresses.

IMPORTANT NOTE! This job requires the Memory job to have been run on a Field Extraction to create a 'Memory image'. You can see this Memory image from the EXHIBIT CONTENT tab.

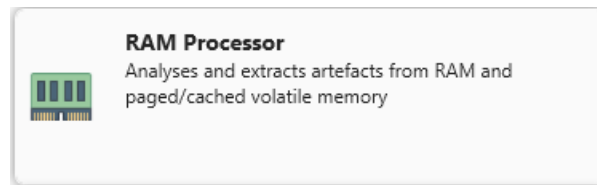
Figure 525



How To Run the Job:

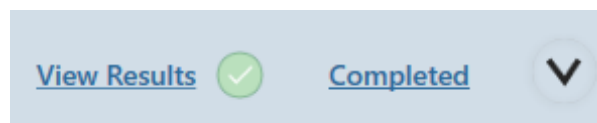
- Select the 'RAM Processor' in the Analytics pop-up window, then select the START button to run the job.

Figure 526



- Once completed, you should see a lot of extra data extracted from the RAM Image in the EXHIBIT CONTENT tab; alternatively, you can select VIEW RESULTS to go straight to EVIDENCE BROWSER with all the files pulled from the job.

Figure 527



GMDSOFT MDF PROCESSOR

The GMDSOFT MDF Processor analytic job reads data from the GMDSOFT MDF file created after an extraction using GMDSOFT MD-NEXT. This analytic can be performed once the GMDSOFT MDF Importer job has been run.

NOTE! Please ensure you have the correct GMDSOFT license applied before attempting this job. Without the license, this process will not function.

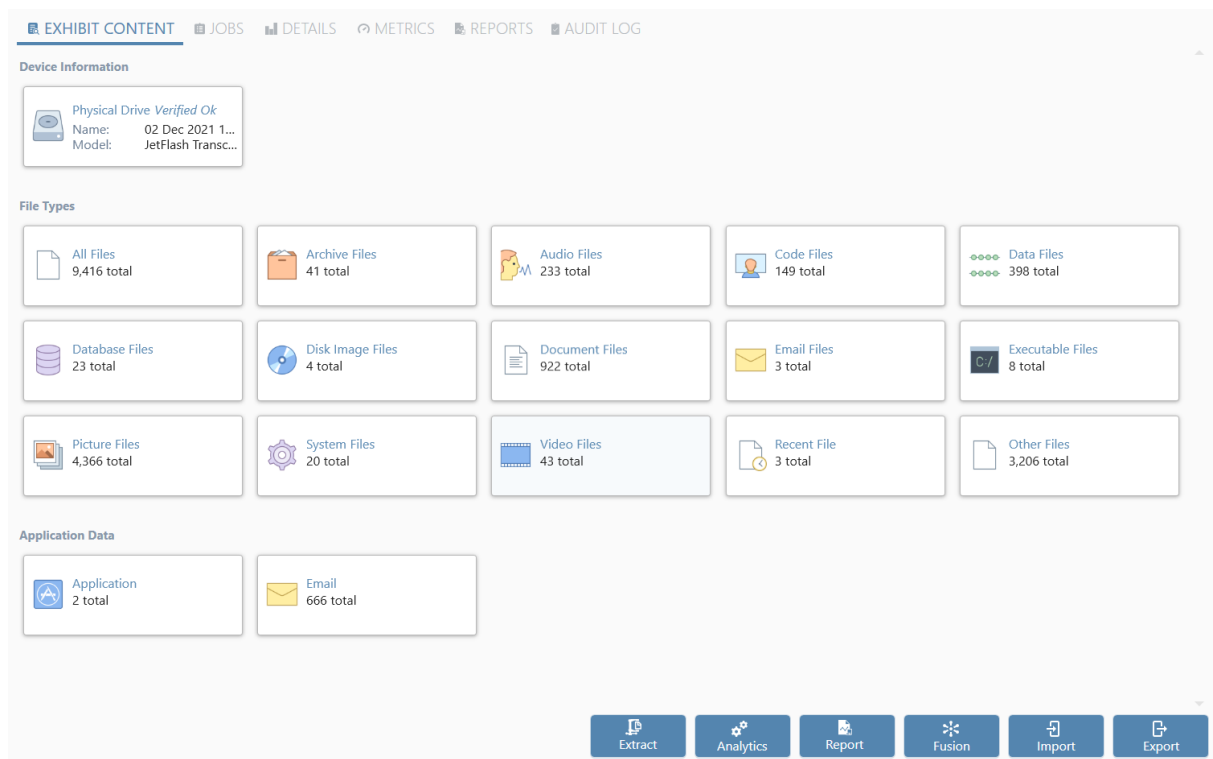
- Select the 'GMDSOFT MDF Processor' in the Analytics pop-up window, then select the START button to run the job.

Figure 528



- Once the job has finished, you can select the VIEW RESULTS button to navigate the evidence browser. You will also see what has been processed in the EXHIBIT CONTENT section.

Figure 529



BITLOCKER PHYSICAL IMAGE DECRYPTER

Decrypts BitLocker partitions in a forensic image or physical disk and creates forensic images from the decrypted partitions for further processing in Detego Analyse. The job supports BitLocker password or BitLocker recovery key.

Figure 530



To run the BitLocker Physical Image Decrypter, follow the below steps:

- From your case list, click on the exhibit you have with the encrypted image. If you right click and select "New Extraction" or select the Extract action tile at the bottom of the screen then it will display the below:

Figure 531



Encrypted Image Detected

Encryption was detected on the disk image you selected.

Disk Encryption Type: **Bitlocker Volume**

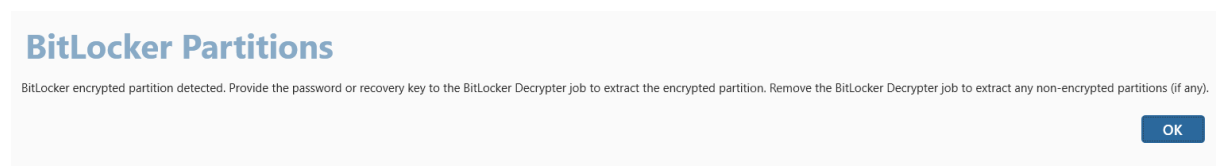
Enter the password or recovery key below to decrypt it for extraction.

Please be aware that if a password is entered then only the encrypted partitions will be extracted.
You may continue without entering a password, in this case only unencrypted partitions will be extracted.

Password or recovery key:

- In order to extract from the encrypted partitions you will need the BitLocker recovery key or password. Enter it in the text box and select CHECK PASSWORD. This will display the below dialog:

Figure 532

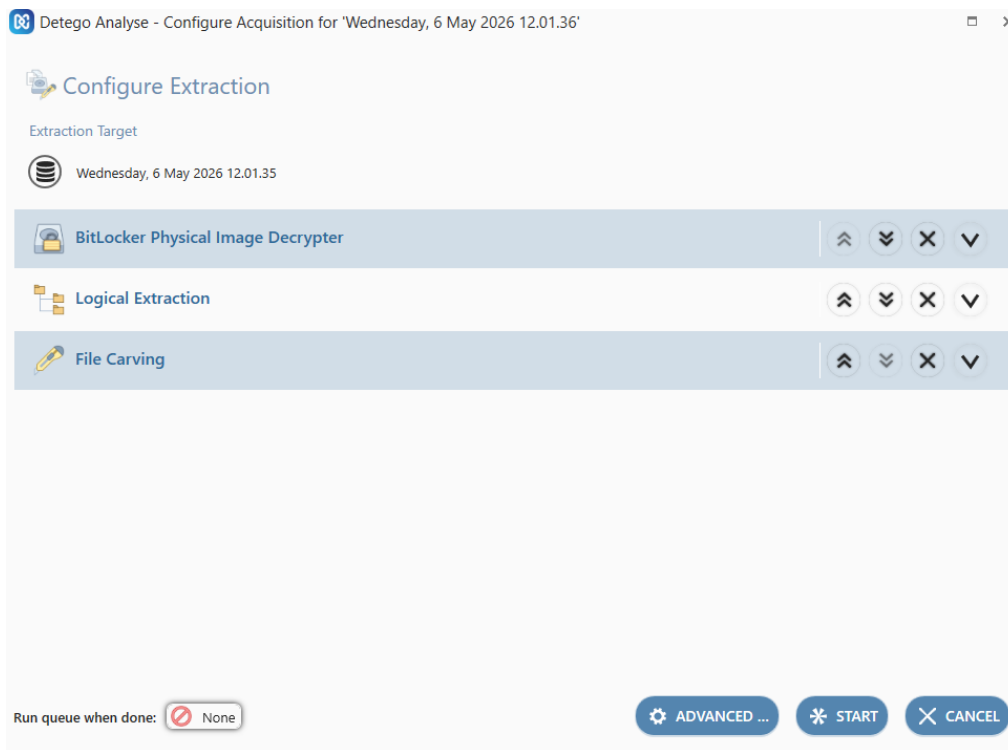


BitLocker Partitions

BitLocker encrypted partition detected. Provide the password or recovery key to the BitLocker Decrypter job to extract the encrypted partition. Remove the BitLocker Decrypter job to extract any non-encrypted partitions (if any).

- Selecting OK will bring you to the Configure Acquisition window with BitLocker Physical Image Decrypter analytic at the top of the queue.
 - Selecting the analytic will expand to show the BitLocker Physical Image Decrypter details. See the section below.

Figure 533



Alternatively, you can do the following:

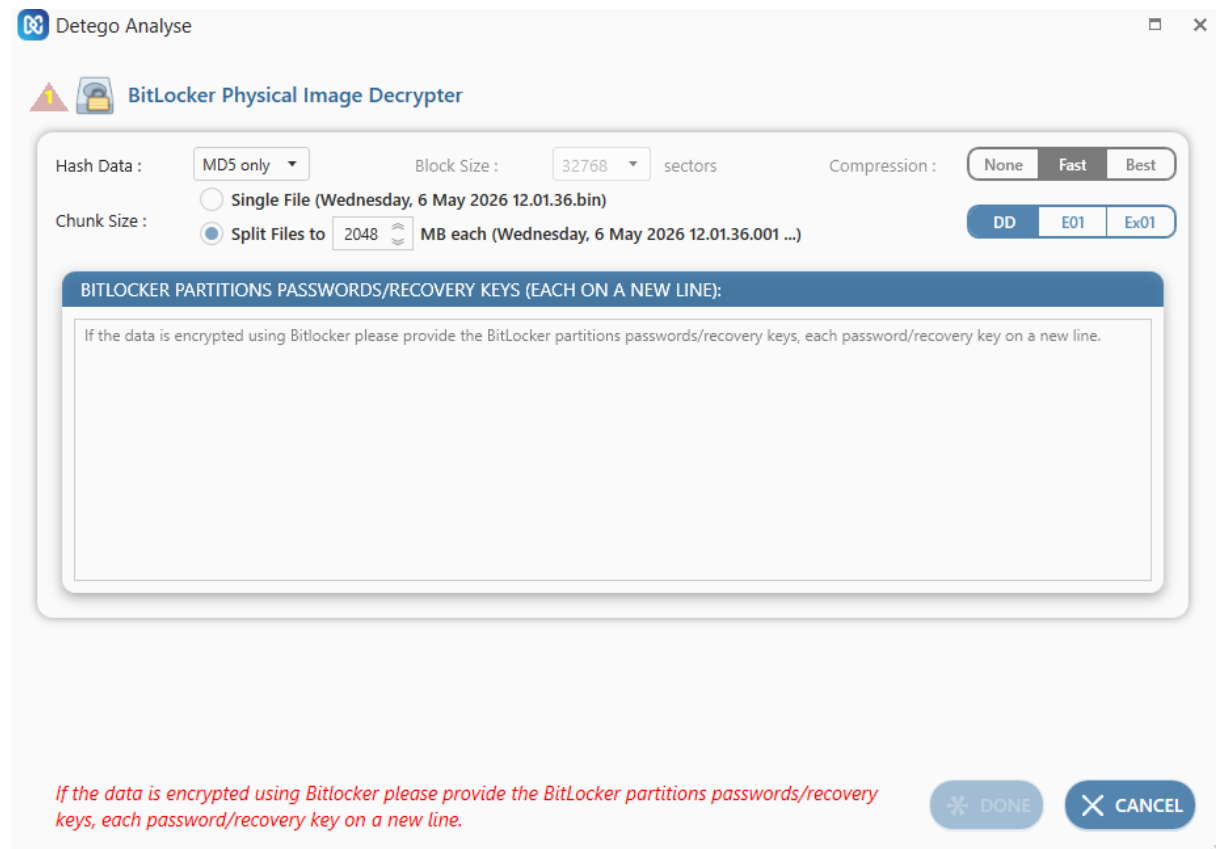
- Select the exhibit that contains the encrypted image
- Select the Analytics tile at the bottom (or right click the exhibit and select New Analytic)
- Select the BitLocker Physical Image Decrypter analytic

Selecting the analytic will open the details of that analytic allowing you to adjust aspects of the job:

- Hash data - specifies the data hash (MD5, MD5 and SHA1, or MD5 and SHA256)
- Block size - sets the block size in sectors (unavailable for DD)
- Compression - specifies the compression method, if any (unavailable for DD)
- Chunk size - allows selection of single or split files with configurable chunk sizes.
- DD/E01/Ex01 - allows you to select which image type to decrypt as.

Provide the BitLocker partition passwords or recovery keys. Each password or recovery key must be on a new line, before selecting DONE.

Figure 534



TEXT INDEXER

The Text Indexer engine indexes the locations of words and phrases within an item of evidence (including text from documents, emails, and images that have OCR run on them). It creates a copy of the indexed data for future searches, making it possible to achieve near-instantaneous results when keyword matching.

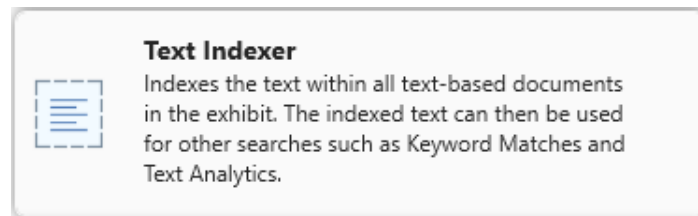
The investigator can configure the granularity of the indexing process by choosing only to index documents, operating system files, messages, or internet files.

To run the 'Text Indexer', follow these steps:

- Open the 'Analyse and Manage' module and select the exhibit you wish to index.
- Click on the 'Analytics' button along the bottom bar, OR right-click on the exhibit and select 'New Analytic' from the dropdown.

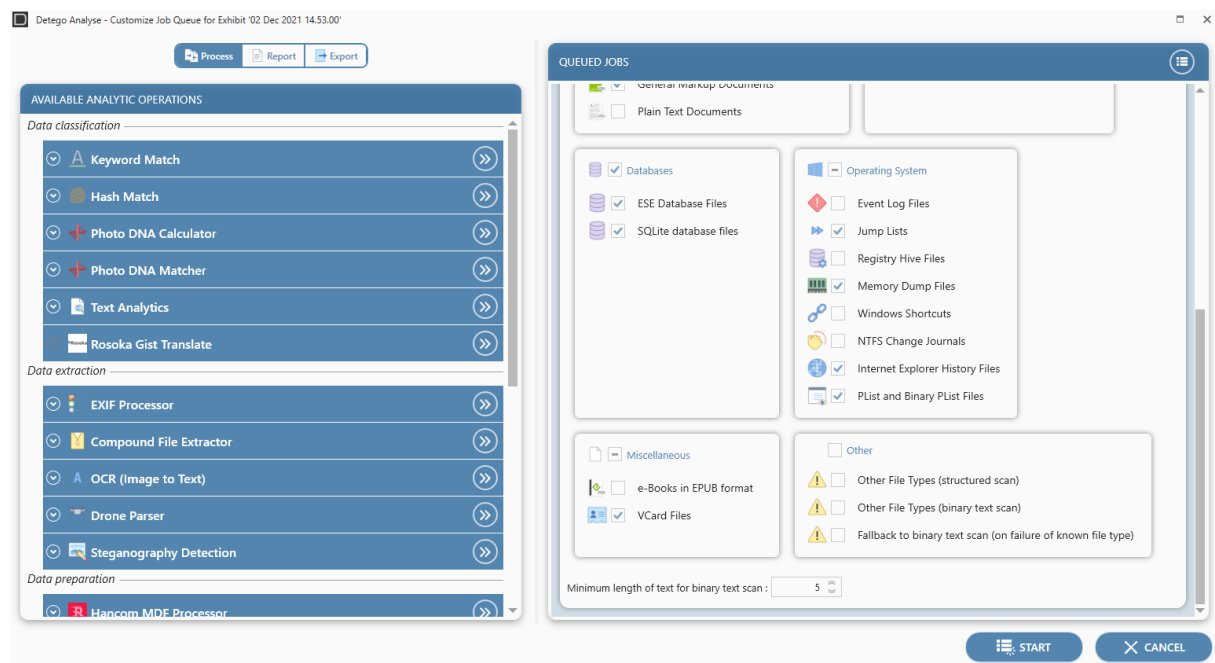
- Select the 'Text Indexer' button from the 'Data Preparation' title to highlight it; a green tick will appear on the right.

Figure 535



- If you'd like to customise the process, click the 'ADVANCED...' button for additional indexing options. In the 'Customise Job Queue' pop-up, expand 'Text Indexer' in the 'Queued Jobs' column to reveal a list of configurable fields. Toggle the slide-on buttons to enable and disable the indexing of different artefacts and move the 'Search timeout' field to adjust the search time.

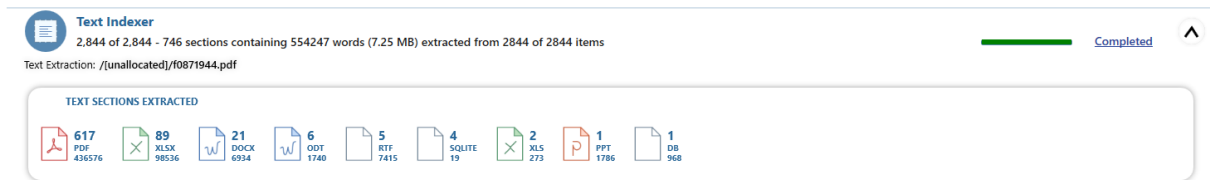
Figure 536



The "Minimum length of text for binary text scan" counter allows you to set the minimum text length for a binary string search, which only applies when the binary text scan options are enabled. These items are marked by a warning triangle in the 'Other' panel. Changing this to a lower number will increase the time taken.

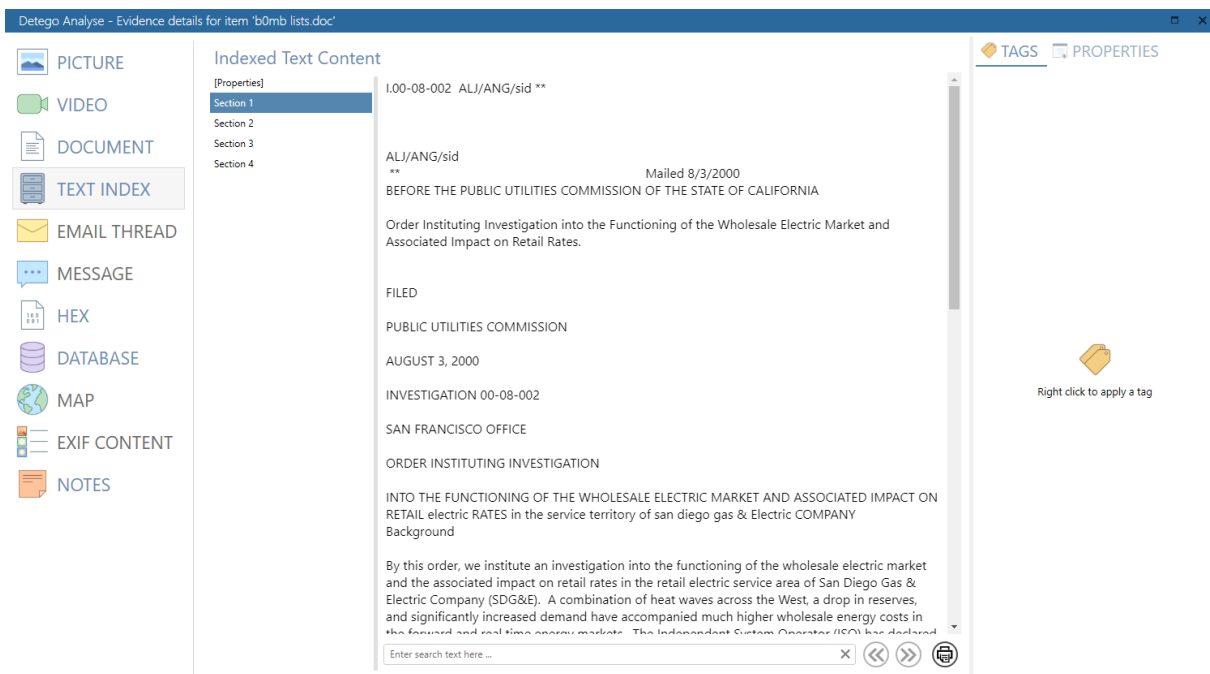
- Click on the 'START' button at the bottom of the pop-up. Indexing should run until completion.

Figure 537



- After the 'Text Indexer' process has run, keyword matching and other analytical processes can be performed against the indexed text strings and phrases.
- Once Text Indexer has been run on the selected items, you can view the indexed text by clicking View Results and opening an item. This will bring you to the 'TEXT INDEX' tab in the Omniviewer.

Figure 538



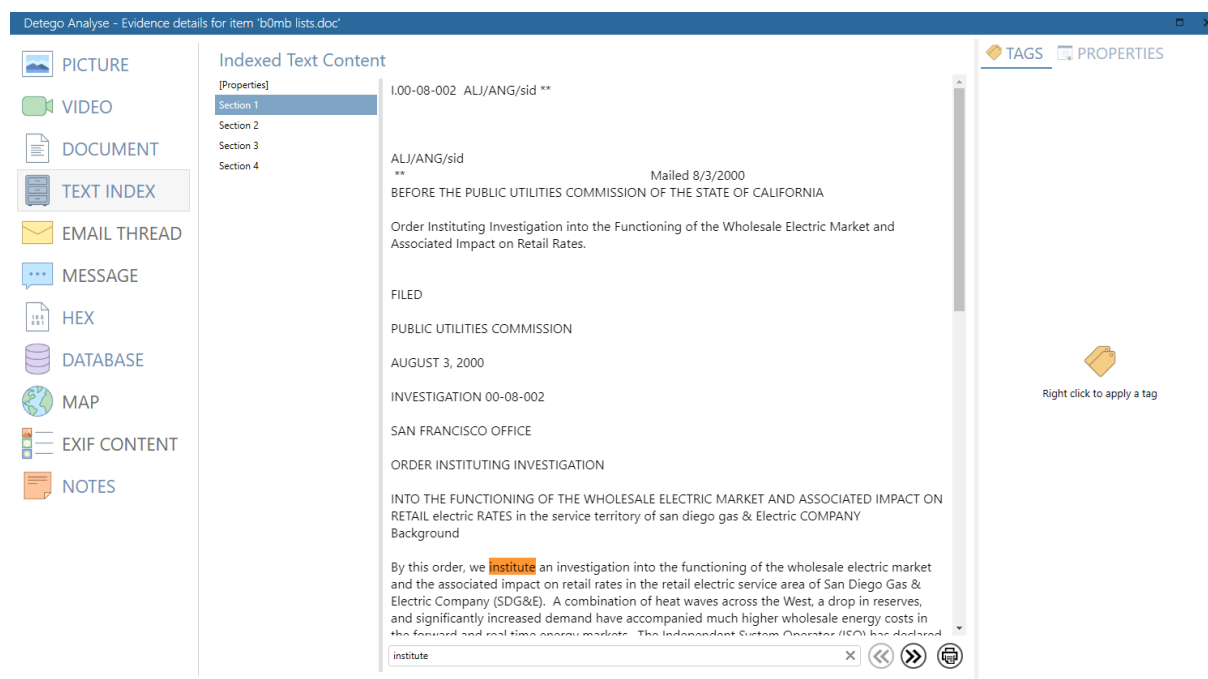
WILDCARDS AND FULL REGEX

After text Indexing a document, you can search within each section for words, wildcards or RegEx (Regular Expressions).

WORD SEARCHING

The most straightforward thing is to type the word you wish to search for in the search bar at the bottom of the TEXT INDEX window.

Figure 539

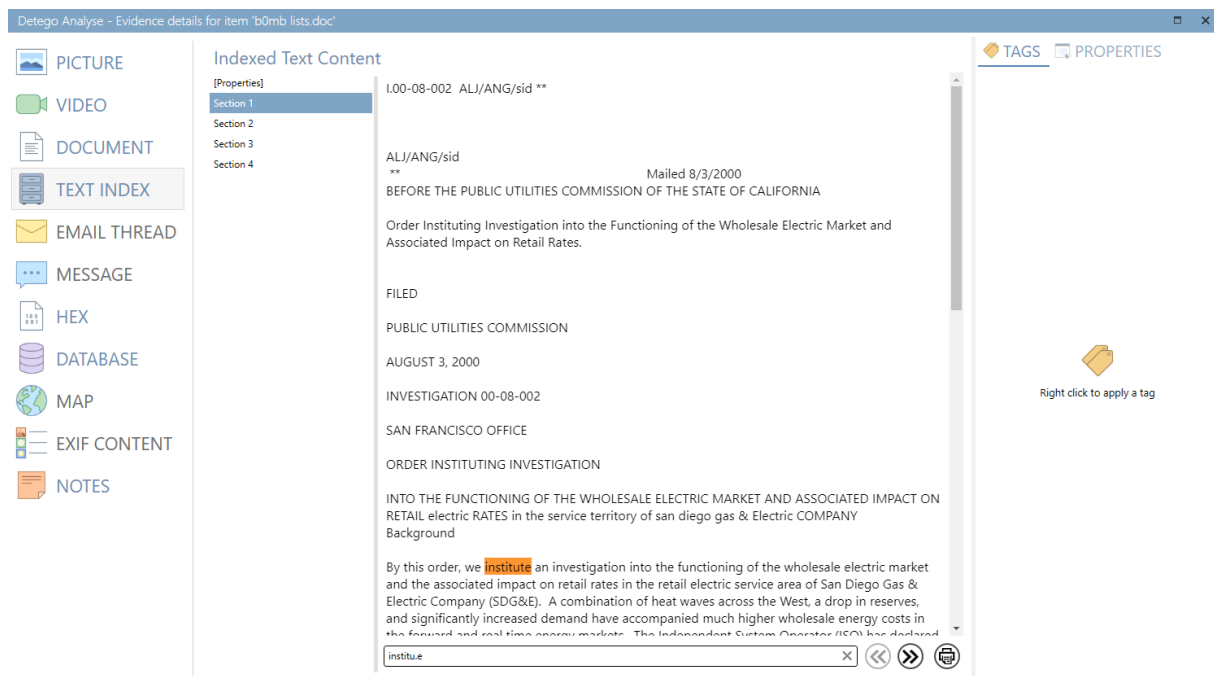


WILDCARDS

Similar to basic word searching, however, it involves special characters representing different things. The characters include the following (characters are within the square brackets below):

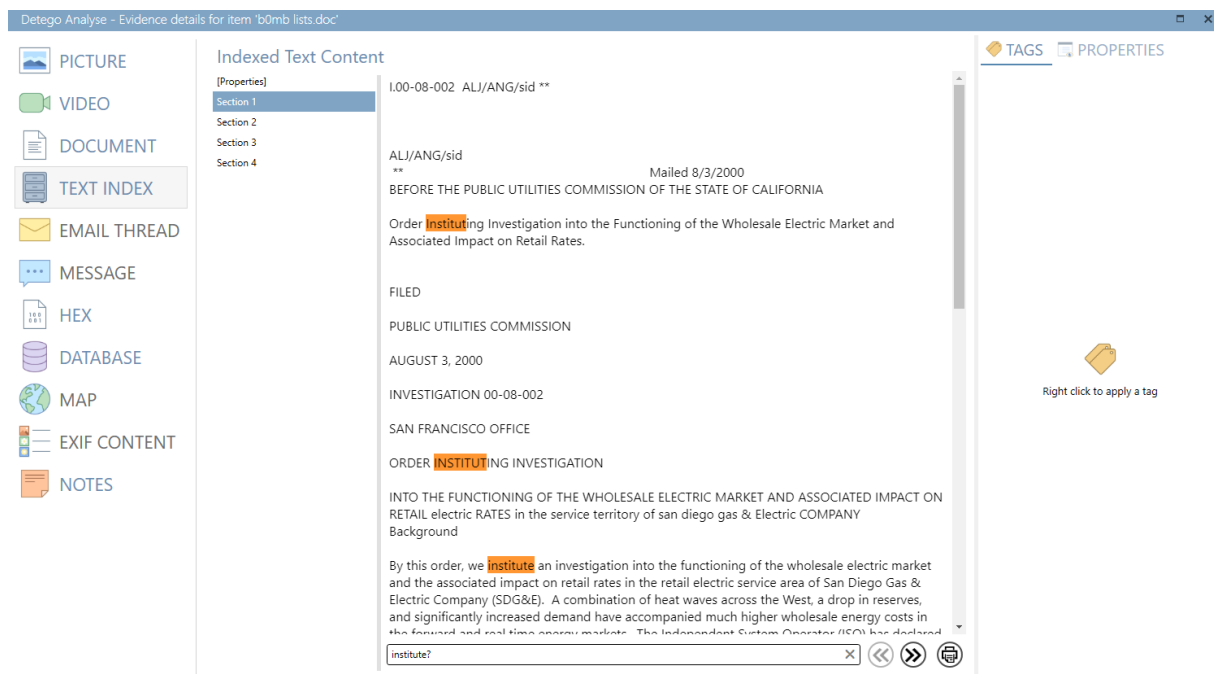
- [.] – Matches any single character except the new line character (\n), e.g., "ra.n" will match "rain" "real" and "raul."
- [?] – Matches the last element 0 or one times. e.g., "rai?n" will match "rai", "rain" and "rain."
- [*] – Works similar to the [?] except that it matches 0 or more instances of the preceding character.

Figure 540



- [.] – In the above example, “institu.e” is typed in the search box, meaning that the word institute is matched as the '.' takes the place of any single character.
- [?] – In the example below, you can see "institute?" is typed in the search box, meaning that the word institute will be matched, as well as the character before "institut."

Figure 541



FORENSIC IMAGE VERIFICATION

After an acquisition, the 'Forensic Image Verification' process checks the image's integrity by comparing the original media's hash value(s) with the resultant forensic image in either E01 or DD format.

Note: This process is only necessary if the verification option wasn't toggled on before the operator began the acquisition.

To perform a 'Forensic Image Verification', follow these steps:

- Select the 'Forensic Image Verification' button under the 'Data Preparation' title.
- In the 'Forensic Image Verification' pop-up, select either the 'All images', 'All unverified images' or 'Selected images' radio button and toggle the 'Verify?' field so it turns green. Click the 'DONE' button in the bottom right corner to begin the process.

Figure 542

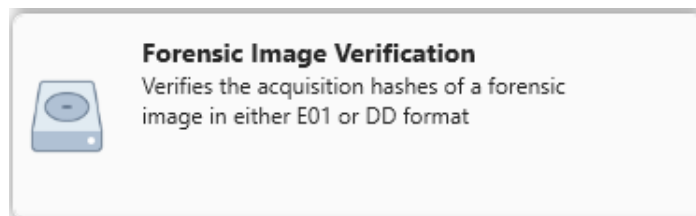
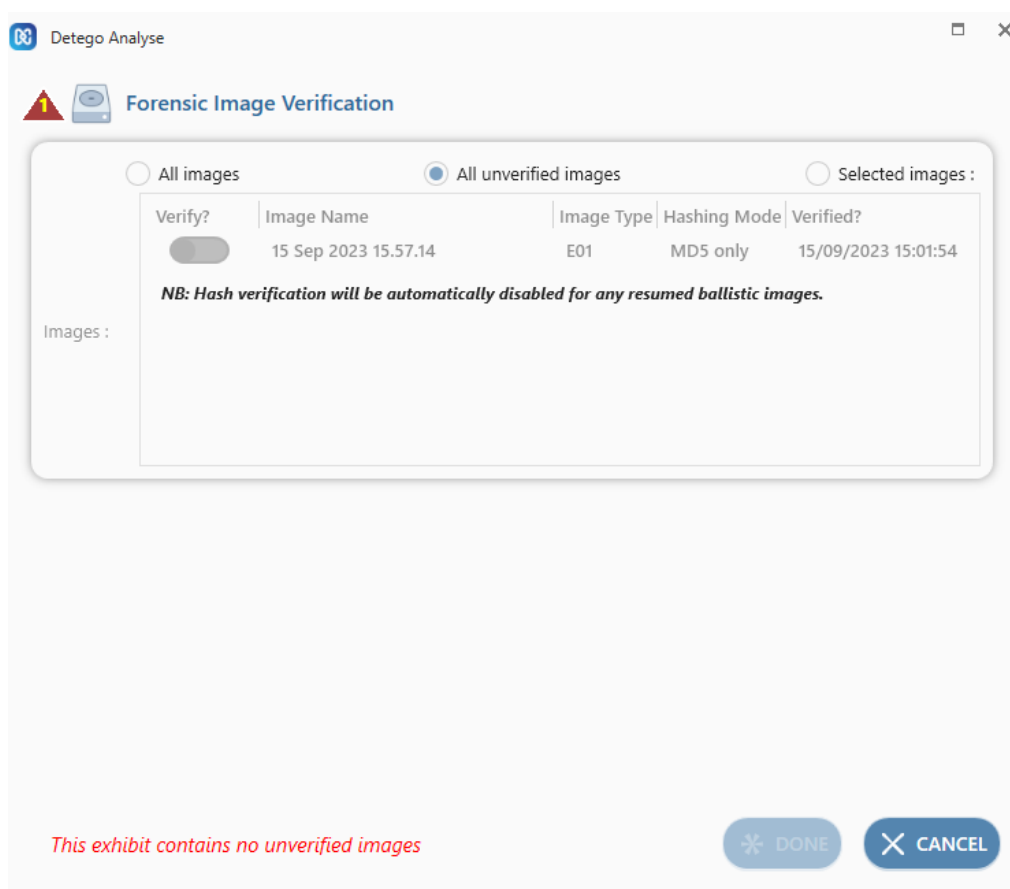
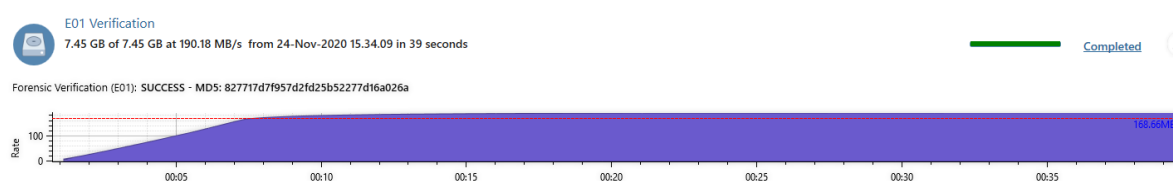


Figure 543



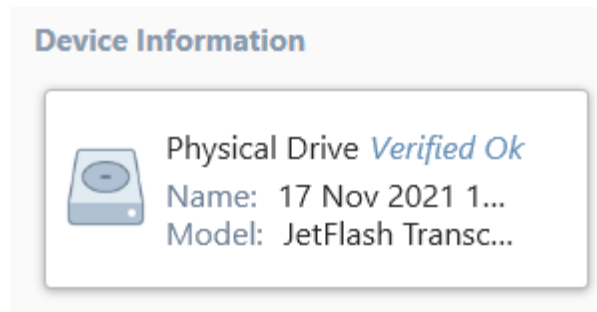
- Return to the 'Analytics' pop-up and click on 'START'. The verification should run until completion. Below is how this process is viewed in the 'Jobs' tab.

Figure 544



- Once the process has finished, the 'Physical Drive' tile in the 'Exhibit Content' tab will be tagged as 'Verified' if the verification is successful or 'Failed Verification' if it fails.

Figure 545



ANALYSE APP DATA

The 'Analyse App Data' process reads through the exhibit content, identifying files and databases and mapping them with their associated applications. Once the process has finished, the mapped data and associated applications are displayed in a readable format in the Evidence Browser within the 'Exhibit Content' tab.

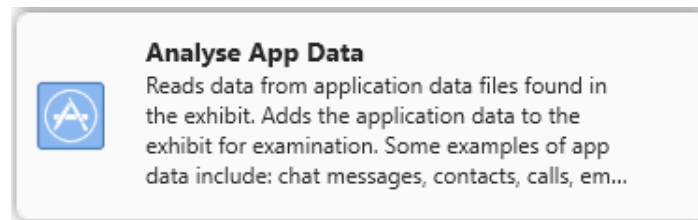
Common artefacts associated with this module include address books, call history, URLs, SMS, emails, browser history, chat history, media files, documents, calendar events, maps, GPS locations, credit card information and social networking data. The achieved results may vary depending on the type of exhibit.

Once this analytical process has been run, the information becomes accessible for examination using the platform's many other analytical processes and keyword searches.

To 'Analyse App Data', follow these steps:

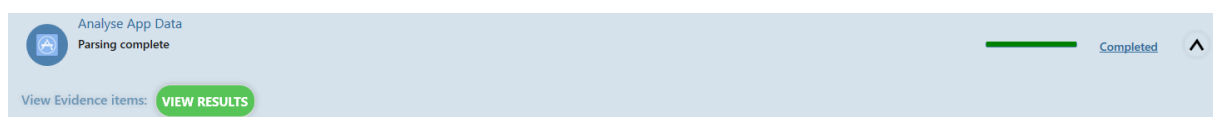
- Open the 'Analyse and Manage' module and select the exhibit you wish to analyse.
- Click on the 'Analytics' button along the bottom bar, OR right-click on the exhibit and select 'New Analytic' from the dropdown.
- From the 'Data Preparation' title, select the 'Analyse App Data' button to highlight it; a green tick will appear on the right.

Figure 546



- Click on the 'START' button at the bottom of the pop-up. The analysis should run until completion.

Figure 547



- The extracted data is parsed and viewable from the 'Exhibit Contents' tab.

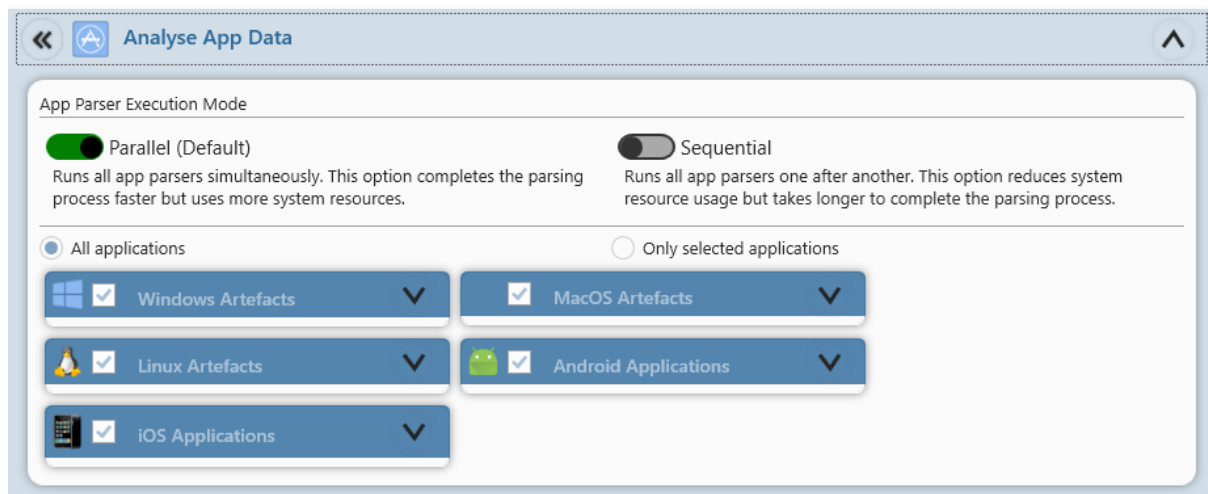
APP PARSER EXECUTION MODE

The App Parser Execution Mode is a feature that provides users with the flexibility to choose how parsers are executed within Detego Analyse. Users can now select between two modes: Parallel (default) and Sequential.

HOW IT WORKS

Upon selecting the App Parsing process, users will be presented with an option to select the execution mode, as shown in the figure below.

Figure 548



Parallel (Default):

In this mode, all parsers are executed simultaneously. This approach leverages multi-threading to speed up the overall parsing process.

- **Faster Completion:** The primary advantage of this mode is speed. By running multiple parsers at the same time, the total time required to complete the parsing process is significantly reduced.
- **Efficiency in High-Powered Systems:** Systems with multiple cores and high computational power can handle parallel processing more effectively, utilising available resources to their full potential.

Sequential:

In this mode, parsers are executed one after another in a defined sequence. This approach ensures that only one parser runs at any given time.

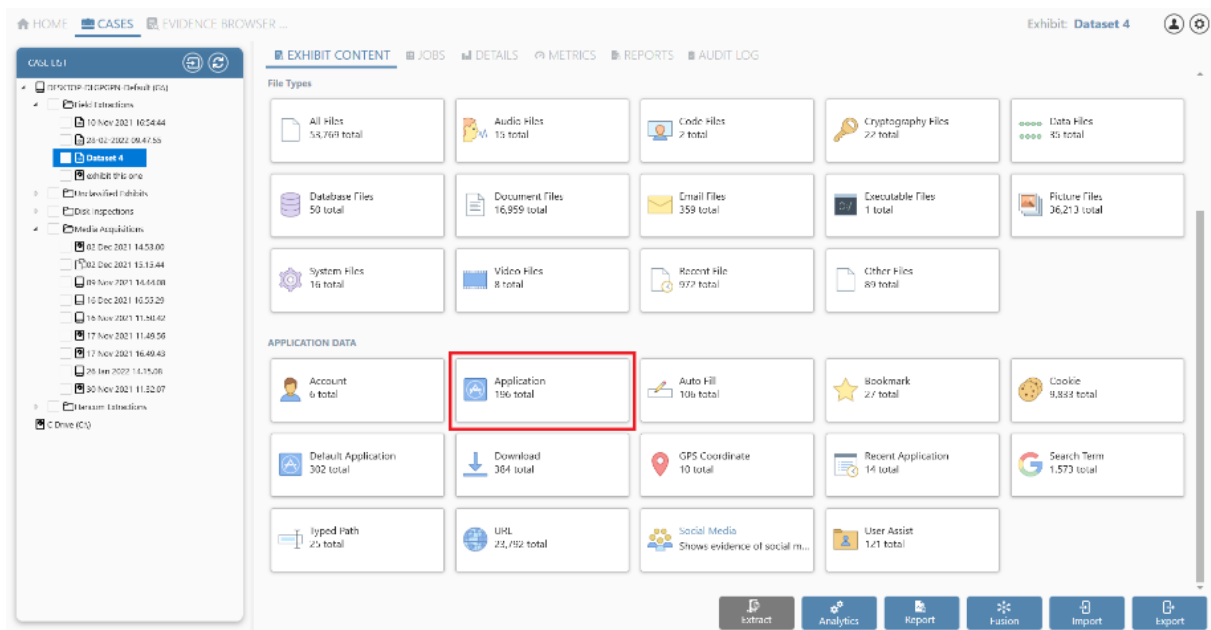
- **Reduced Risk of Conflicts:** By running parsers one after another, the risk of resource contention and conflicts between parsers is minimised, potentially leading to more reliable parsing outcomes.
- **Slower Completion:** The main drawback is the time required to complete the parsing process. Sequential execution is inherently slower as it does not leverage the benefits of parallel processing.

- **Underutilisation of High-Powered Systems:** Systems with high computational power may not be fully utilised in this mode, leading to inefficiencies.

HIERARCHY VIEW

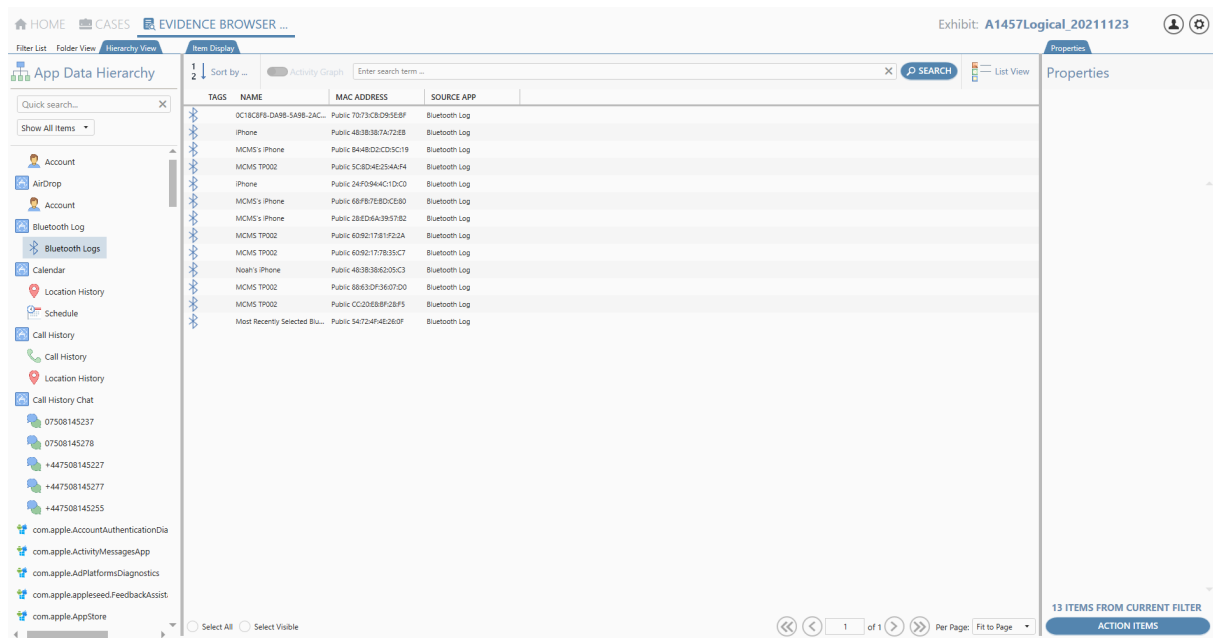
The Hierarchy View is specific to App Data (Applications). To see this, select the exhibit with the Application Data you wish to view and then select the 'Application' tile from the Exhibit Content tab.

Figure 549



Once in the EVIDENCE BROWSER, you can see the 'Hierarchy View' on the left of the window.

Figure 550



You can select the dropdown at the top to choose between:

- Show All Items – This will display all items available
- Hide Empty Items – This will hide any empty items that are visible
- Show Empty Items Only – This will display only the empty items available

FILE HEADER CHECKER

Header information is embedded into every document to identify its file format, for example, Microsoft Word, Excel or PowerPoint. This information is supposed to correspond with the extension generated when a file is saved from its authoring software; however, it is a relatively simple process to change it to conceal the content of a file manually. For example, a Word document extension changed from a .docx to a .mp4.

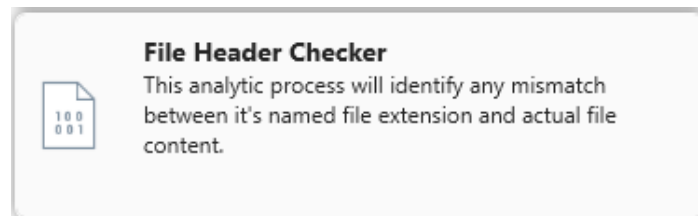
The 'File Header Checker' analytics process scans the content of an exhibit's files against their corresponding file extensions, flagging any discrepancies in the Evidence Browser.

To run the 'File Header Checker', follow these steps:

- Open the 'Analyse and Manage' module and select the exhibit you wish to check.

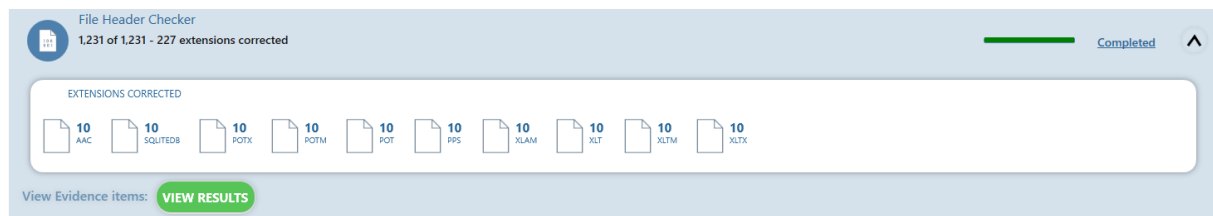
- Click on the 'Analytics' button along the bottom bar, OR right-click on the exhibit and select 'New Analytic' from the dropdown.
- Select the 'File Header Checker' button from the 'Data Preparation' title to highlight it; a green tick will appear on the right.

Figure 551



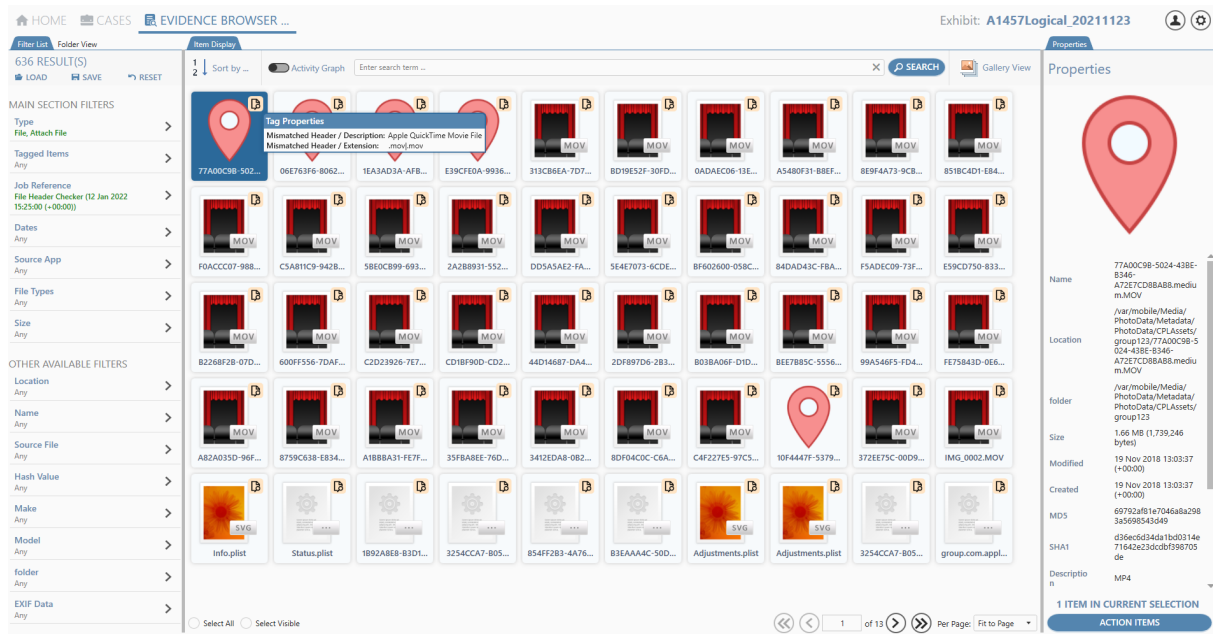
- Click on the 'START' button at the bottom of the pop-up. The check should run until completion; its progress can be viewed in the 'Jobs' tab, with the red labels representing the number of mismatched files found.

Figure 552



- Once the extracted data has been parsed, you can view, examine, analyse, filter and tag the files from the 'Exhibit Content' tab.
- Apply a filter to display only the mismatched files by clicking on the 'Files' button in the 'Exhibit Content' tab to open the 'Evidence Browser'. Then, toggle the 'Tagged Items' field, select 'Show items with selected tags' and expand 'System'. Only tick the 'Mismatched Header' option to view the files with erroneous extensions.

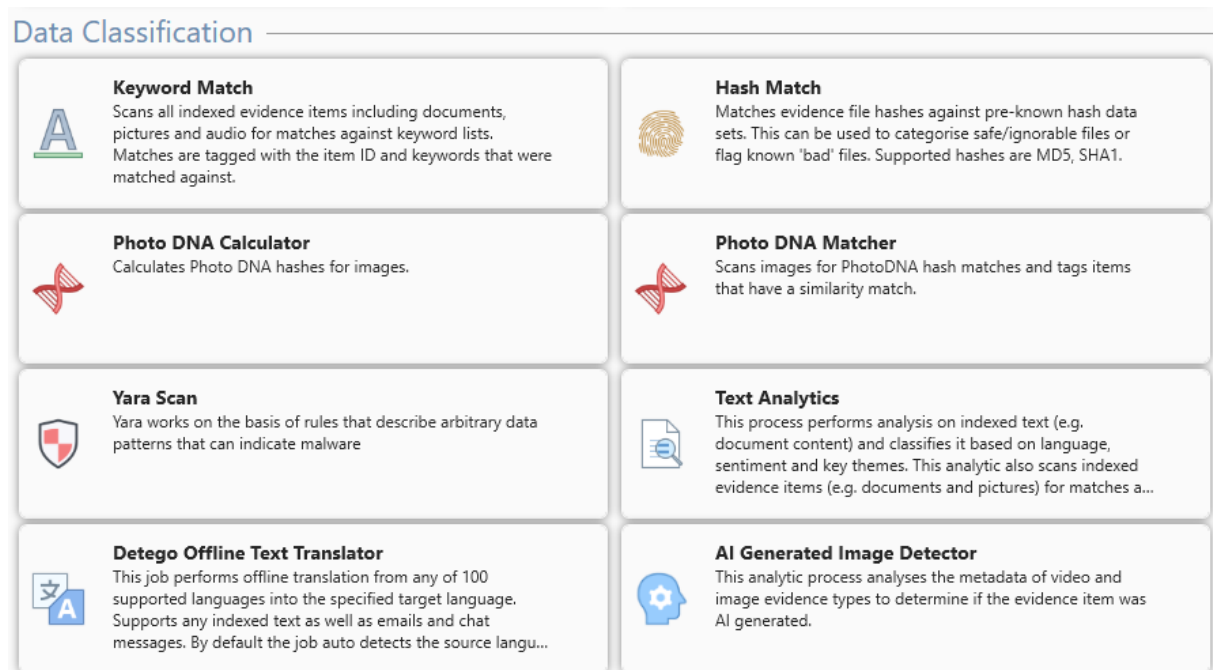
Figure 553



6.12. DATA CLASSIFICATION ANALYTICS

The Data Classification Analytical Process Section consists of jobs classifying the data for further processing.

Figure 554



KEYWORD MATCH

The 'Keyword Match' process identifies potentially critical evidence by running chosen, preconfigured lists of keywords against an exhibit's file names and content (including documents, pictures and audio). Although keyword matching can be done before text indexing, it's advisable to do it after to speed up the investigative process.

Regular expressions (RegEx) can also be added to keyword lists to look for specific strings containing alphanumeric characters or complicated patterns in text. Positive keyword matches are categorised and flagged in the 'Evidence Browser'.

Note: You must have a preconfigured keyword list in the system to perform keyword matching.

To add new keywords and lists, refer to Keyword Lists.

To perform a 'Keyword Match', follow these steps:

Figure 555

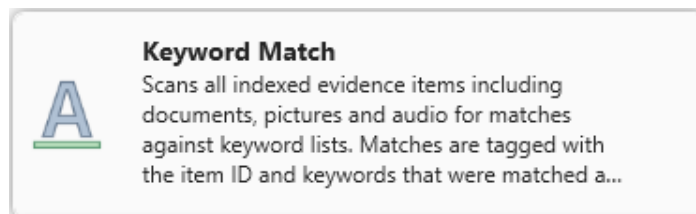
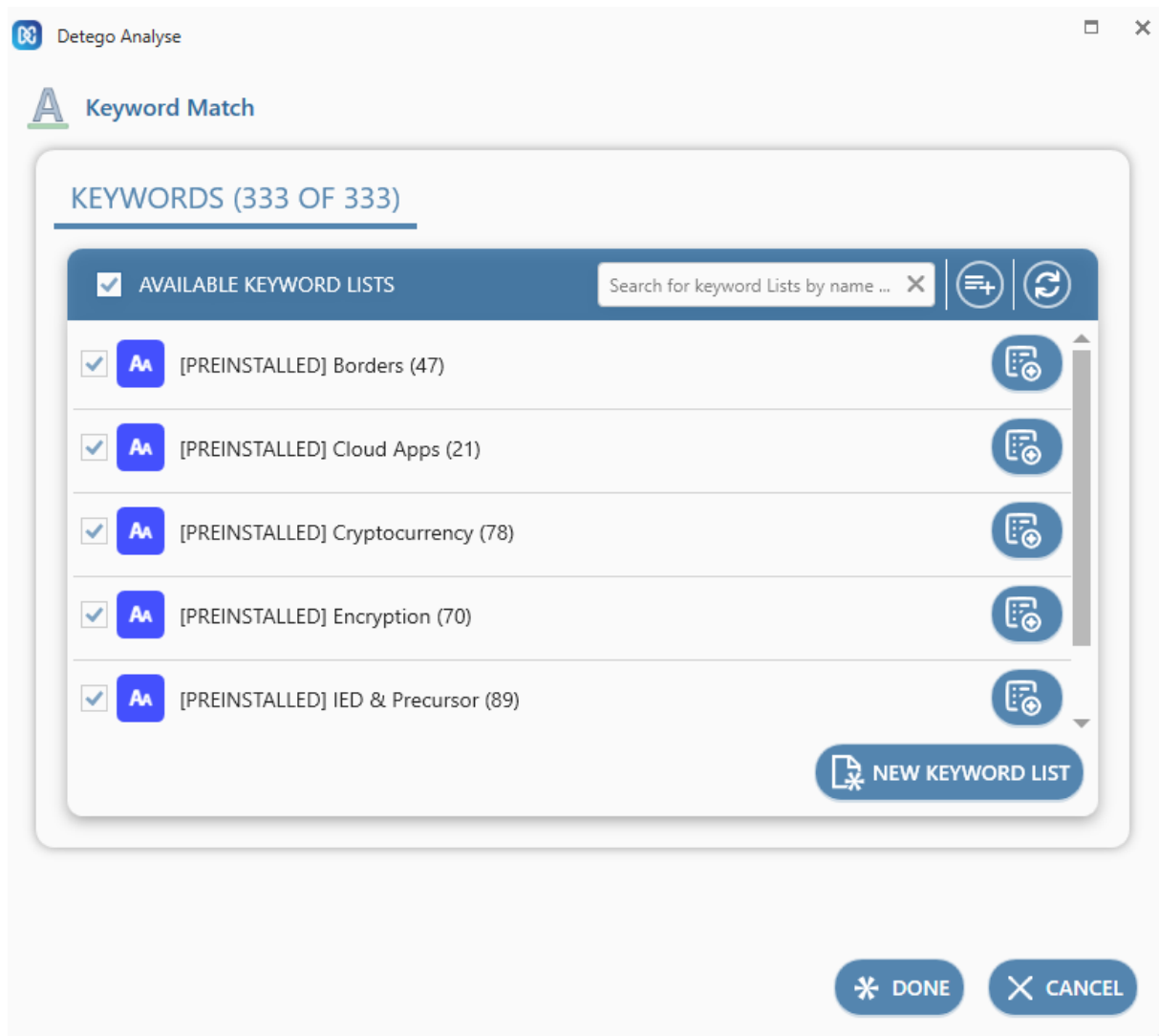


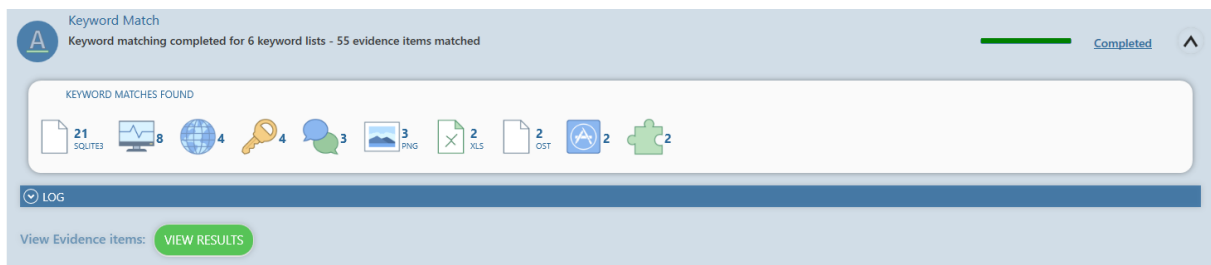
Figure 556



- Select the preconfigured keyword lists to run against the exhibit in the 'Keyword Match' pop-up. Lists can be created by clicking the 'NEW LIST' button at the bottom of the 'AVAILABLE KEYWORD LISTS' column or clicking 'MANAGE' and then 'Import Into List'. Click the 'DONE' button in the bottom right corner to begin the process.
- Return to the 'Analytics' pop-up and click on 'START.' The search should run until it is complete.

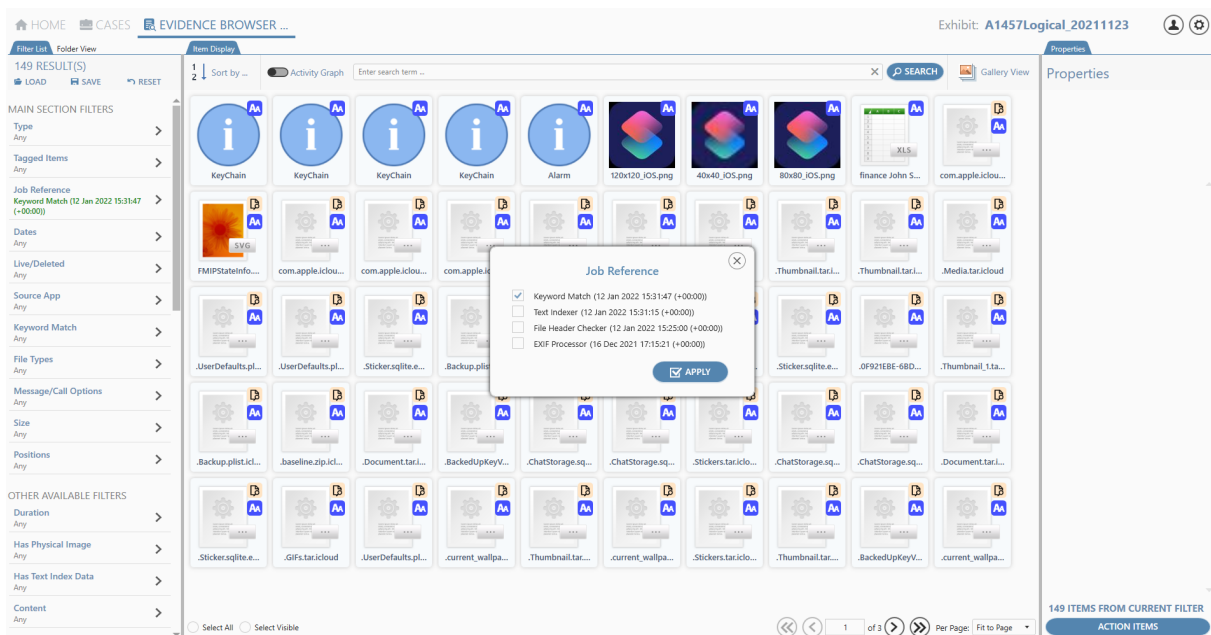
Below is how this process is shown on the 'Jobs' tab.

Figure 557



- Upon completion, you can select the 'VIEW RESULTS' button to go straight to the Evidence Browser with the 'Job Reference' filter selected for the right job.

Figure 558



HASH MATCH

The 'Hash Match' process searches for matches between an exhibit file hashes (the Detego Platform supports MD5 and SHA1) and preconfigured lists of known 'bad' file hashes, e.g., malware, leaked documents, bootlegged software, incriminating files, viruses, etc.

Positive hash matches are categorised and flagged in the 'Evidence Browser'.

Note: To perform hash matching, you must have a preconfigured hashlist in the system. To add new hashes and lists, refer to CONFIGURING HASHLISTS.

To perform a 'Hash Match', follow these steps:

- Open the 'Analyse and Manage' module and select the exhibit you wish to search.
- Click on the 'Analytics' button along the bottom bar, OR right-click on the exhibit and select 'New Analytic' from the drop-down.
- Select the 'Hash Match' button from the 'Data Classification' title.

Figure 559

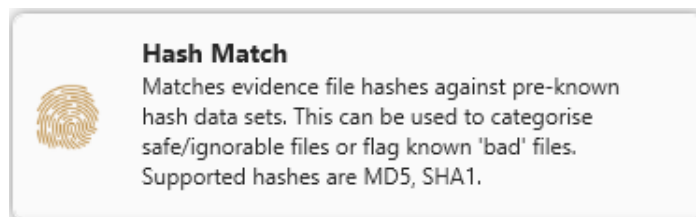
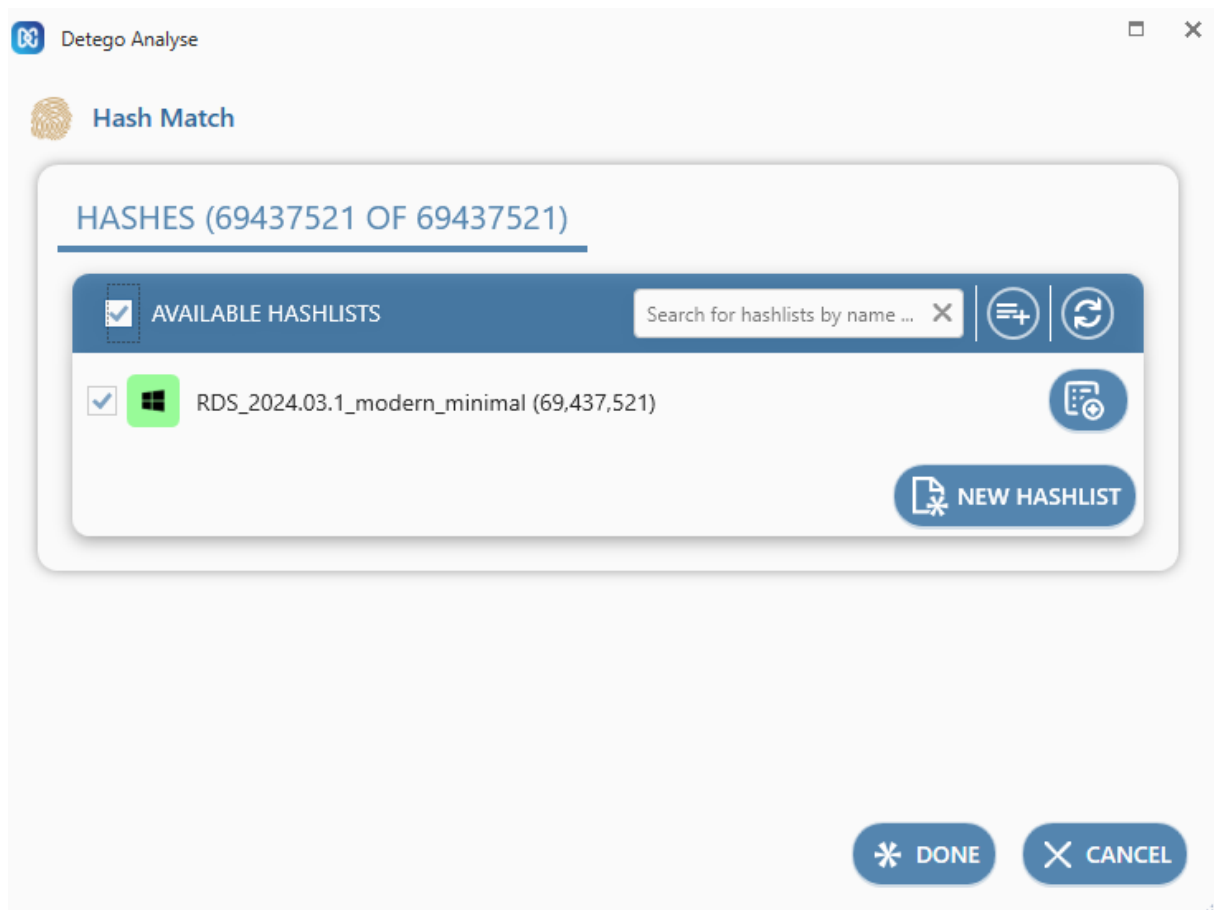


Figure 560



- Select the preconfigured hash lists from the 'Hashes' tab to run against the exhibit from the 'Hash Match' pop-up. Lists can be created by clicking the 'NEW HASHLIST' button at the bottom of the 'AVAILABLE HASHLISTS' column or clicking 'MANAGE' and then 'Import Hashes'.
- Toggle the hashing algorithm fields for MD5 and SHA1 from the 'Options' tab. Click the 'DONE' button in the bottom right corner to begin the process.
- Return to the 'Analytics' pop-up and click on 'START.' The search should run until it is complete.

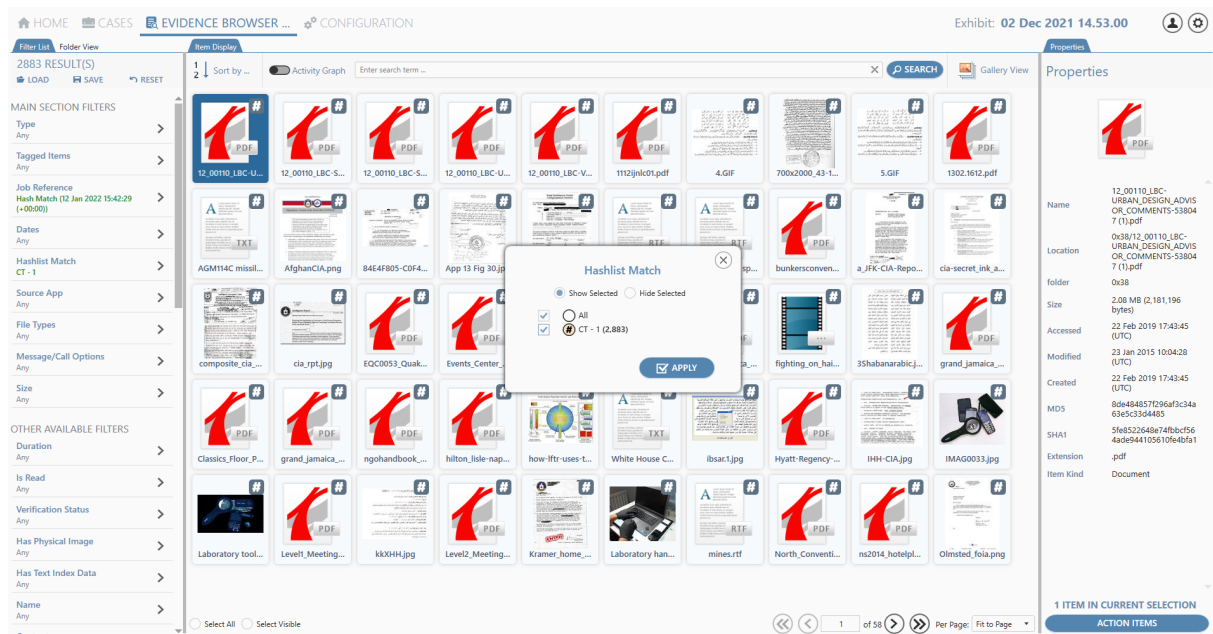
Below is how this process is shown on the 'Jobs' tab.

Figure 561



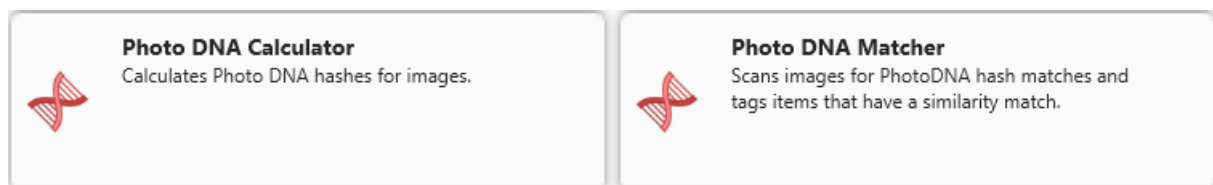
- Upon completion, all files with hash matches are tagged according to the list their hash falls under. Tagged files can be filtered and exported separately.
- Apply a filter to display only the hash-matched files by clicking the 'Files' button in the 'Exhibit Content' tab to open the 'Evidence Browser'. Then, toggle the 'Hashlist' field, select 'Show items which have selected hash matches' and tick the options you wish to view.

Figure 562



PHOTODNA CALCULATOR

Figure 563



Designed by Microsoft to help stop child exploitation images from being shared online, PhotoDNA technology converts images into a common black-and-white format and uniform size, divides the image into squares, and assigns a numerical value representing the unique shading found within each square. Those numerical values represent the hash (unique digital identifier), which can be compared against preconfigured lists of harmful hashes. It's used to find copies of a given image with incredible accuracy, even when the images have been altered.

Hashes are in the following line-separated format: 962da1840a7d90535b247c2d9ea3207d, 213, 544, 112, 029, 776, 114, 220, 211, 221 for example

PhotoDNA calculator will compute PhotoDNA hashes of image files and add the hash to the database.

PhotoDNA Matcher performs the hash matching against selected or all PhotoDNA hash lists.

When the investigator has run a PhotoDNA hash list, the image will be tagged as 'PhotoDNA'.

Detego currently supports jpg, jpeg, png and gif file types.

PHOTODNA MATCHER

The Photo DNA Matcher job scans images for PhotoDNA hash matches and tags items with a similarity match.

The Hash Distance Threshold is set at a default of 41943.03. If you change this figure, select the button next to it to revert to the default.

Testing conducted by Microsoft and confirmed by NCMEC has determined that using the threshold of 41943.03 produces visually identical and visually similar matches with minimal chance for false positives. A value of 0 matches only identical images.

To run the Photo DNA Matcher job, follow the below steps:

- Navigate to the exhibit on which you want to run the Photo DNA Matcher job.
- Select the 'Analytics' button at the bottom of the CASES window, OR right-click the exhibit on the left panel and select 'New Analytic'.
- Select 'Photo DNA Matcher' from the Analytics window under the 'Data Classification' section.

Figure 564

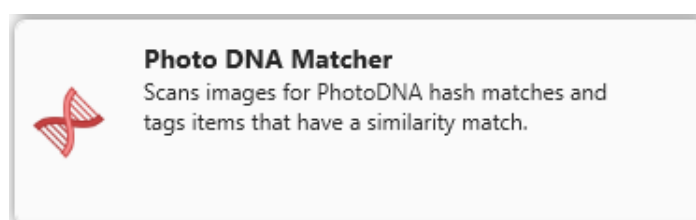
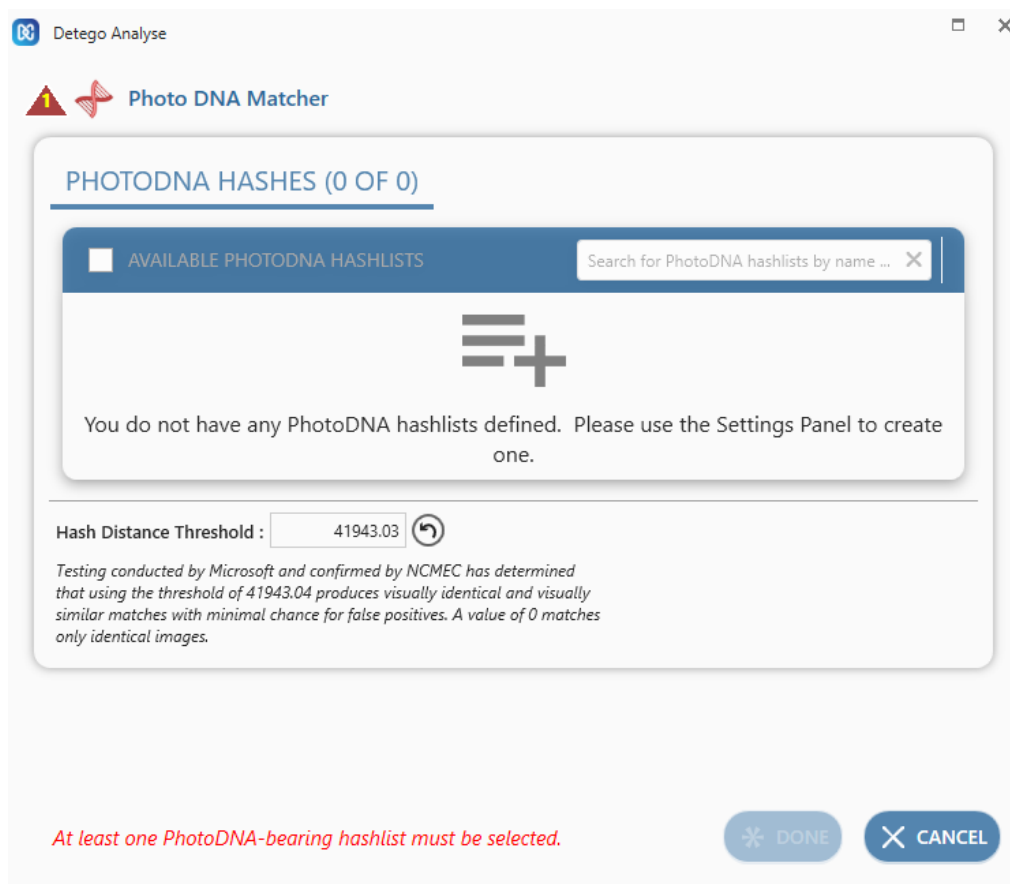
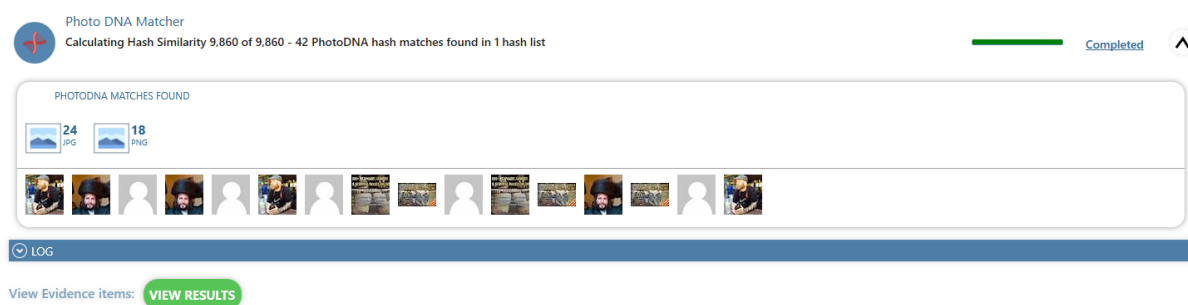


Figure 565



- Select the PhotoDNA Hashlist you wish to run against and adjust the Hash Distance Threshold (if you choose).
- Once ready, select DONE and START to run the job. This will start the job and take you to the JOBS tab.
- Once the job has been completed, you can select VIEW RESULTS to go straight to the EVIDENCE BROWSER and view the matched items.

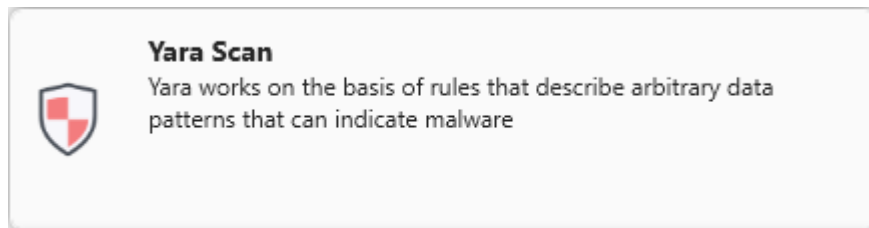
Figure 566



YARA SCAN

The Yara Scan analytic allows you to run a scan against the data/exhibit to match or flag items based on the Yara Rules you select. You can configure your Yara Rule Sets from the Configuration cog in the top right corner.

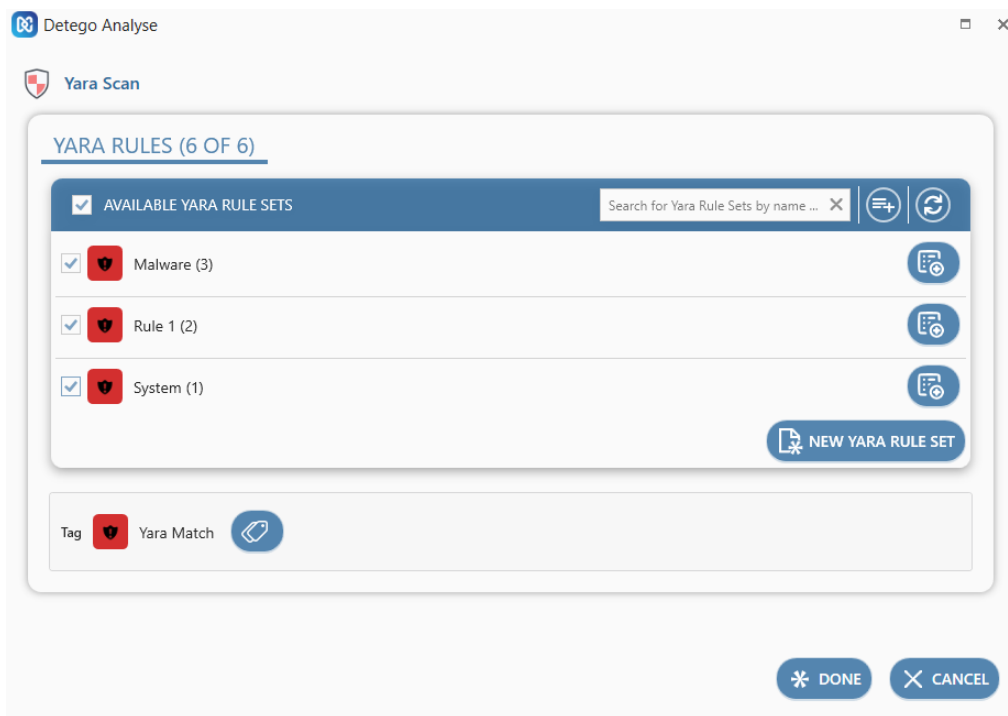
Figure 567



To run the Yara Scan:

- From the Data Classification section in the Analytics window, select the Yara Scan option.

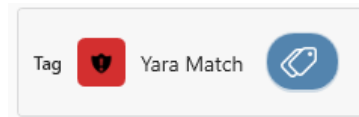
Figure 568



- From the list of Available Yara Rule Sets, select the checkbox on the ones you wish to use for the scan.
 - You can select the Manage icon next to your Yara Rule Set to import, remove or check your Yara Rules for that Rule Set.

- You can select “NEW YARA RULE SET” to create a new Yara Rule Set.
- If you want to change the Tag that any matches will use, select the Edit icon next to the Tag name

Figure 569



- Once you are ready, select DONE and then START to run the analytic.

TEXT ANALYTICS

Text Analytics analyses indexed text (e.g., document content) and classify it based on language, sentiment and key themes.

NOTE! This job requires the **Text Indexing** job to be run beforehand to produce the best results.

There are five options for Text Analytics:

KEY PHRASE ANALYSIS (DOCUMENTS)

Processes document content to determine key phrases in the body of text by analysing the frequency of word appearance and its co-occurrence with other words.

LANGUAGE CLASSIFICATION (DOCUMENTS)

Applies language classification to documents based on the most dominant languages found within the text. Supports 50+ languages.

SENTIMENT ANALYSIS (MESSAGES)

Performs analysis of messages where the content is identified on a positive to negative scale. Messages can then be filtered on the calculated sentiment.

CRYPTOCURRENCY IDENTIFICATION (DOCUMENTS/MESSAGES)

Identifies Bitcoin addresses within the text and extracts them as separate evidence records. Address checksums are validated to remove false positives. Supports Bech32 and Base58 encodings.

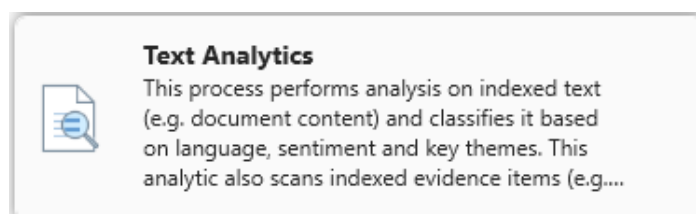
REGULAR EXPRESSION (REGEX) MATCHING

Allows the use of RegEx to search for more specific strings within a document.

To run the Text Analytics job, follow the below steps:

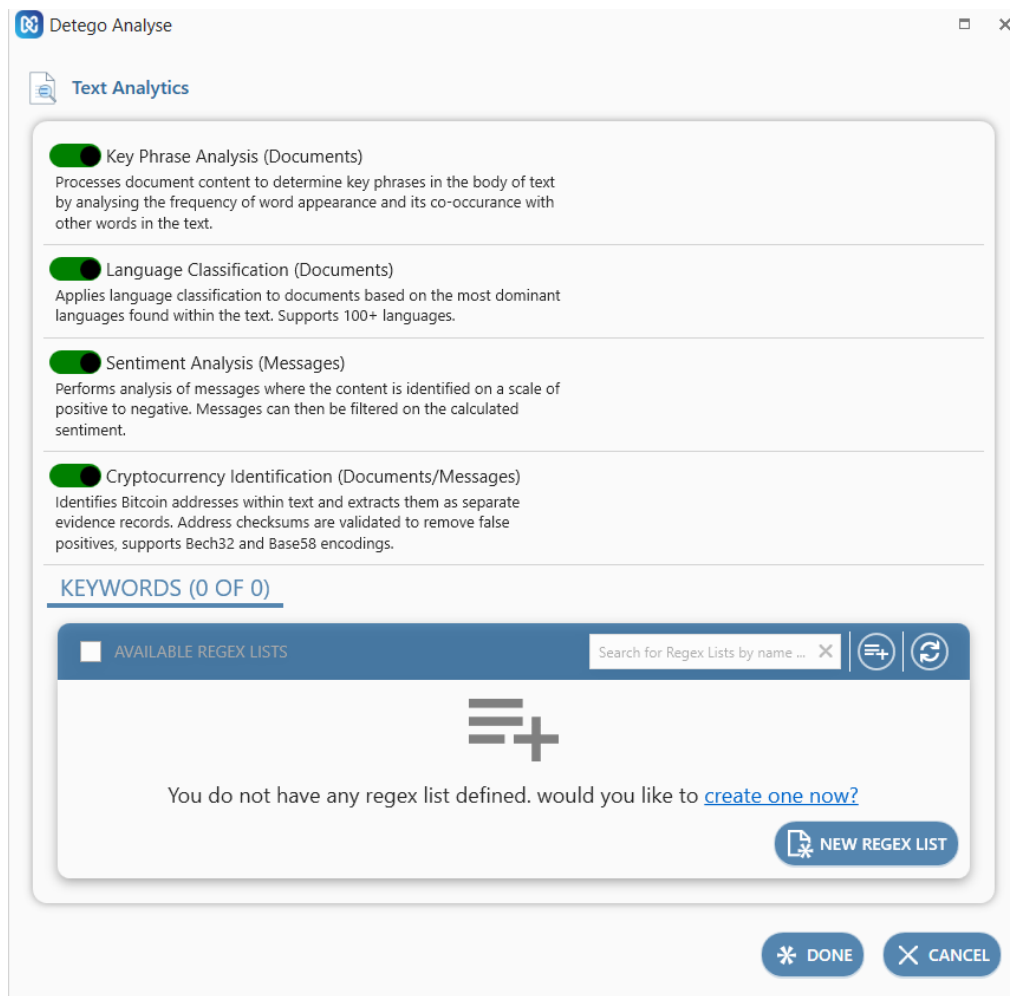
- Navigate to the 'Analyse Manage' section of Detego and select the exhibit you wish to run the analytic on.
- Select the 'Analytics' button at the bottom OR right-click the exhibit on the left CASES panel and select 'New Analytics'.
- Select the 'Analytics' job from the Analytics window under the 'Classification' section.
- Select START to run the default settings OR ADVANCED... to adjust settings.

Figure 570



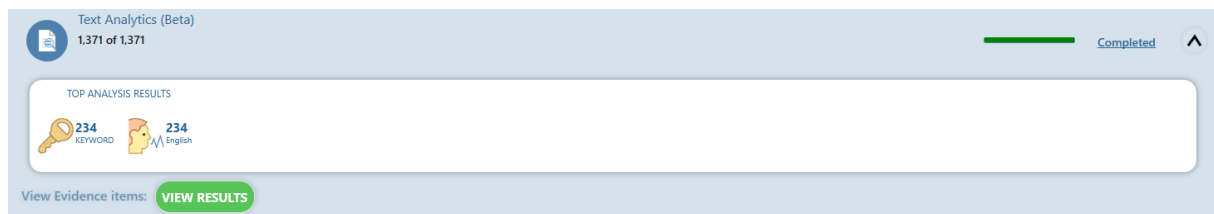
- Select the options you wish to run or input a RegEx string.

Figure 571



- Once you click START, the job will start, and you will be taken to the JOBS tab to view the progress.
- Once the job has been completed, you can select VIEW RESULTS to go straight to the EVIDENCE BROWSER and view the items.

Figure 572



DETEGO OFFLINE TEXT TRANSLATOR

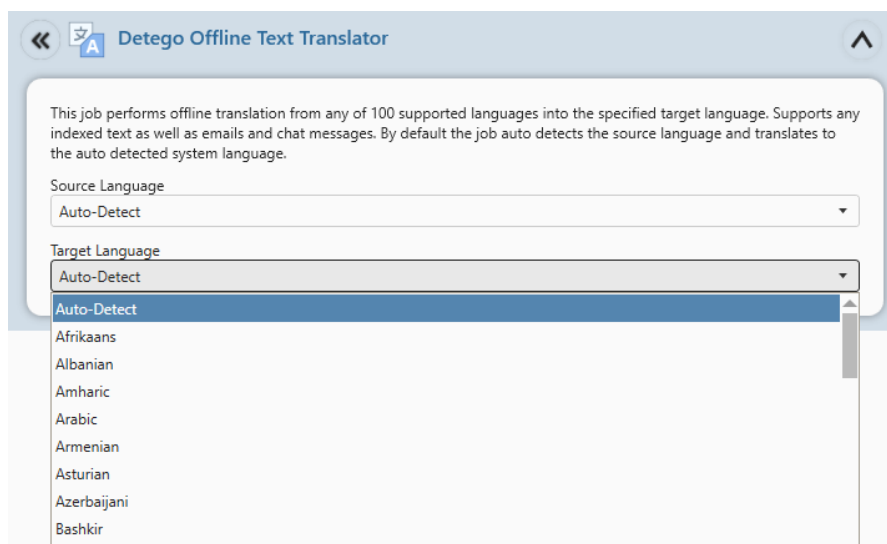
Detego Offline Text Translate will quickly translate non-English documents into any of the 100 languages supported. It can translate between any of these languages, not just to English.

This feature requires an additional license and **will only work after running Text Indexer**.

To run the Detego Offline Text Translator analytic, follow the below steps:

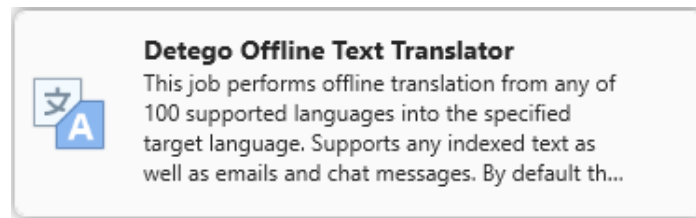
- Navigate to 'the 'Analyse Manage' section of Detego and select the exhibit you wish to run the analytic on.
- Select 'the 'Analytics' button at the bottom **OR** right-click the exhibit on the left CASES panel and select 'New Analytics'.
- Select the 'Detego Offline Text Translator' job from the Analytics window under the 'Data Classification' section.
- Click 'Advanced' to select the Source Language if known and the target language you would like to have translated to.
 - If left unchanged the the 'Auto Detect' will apply.

Figure 573



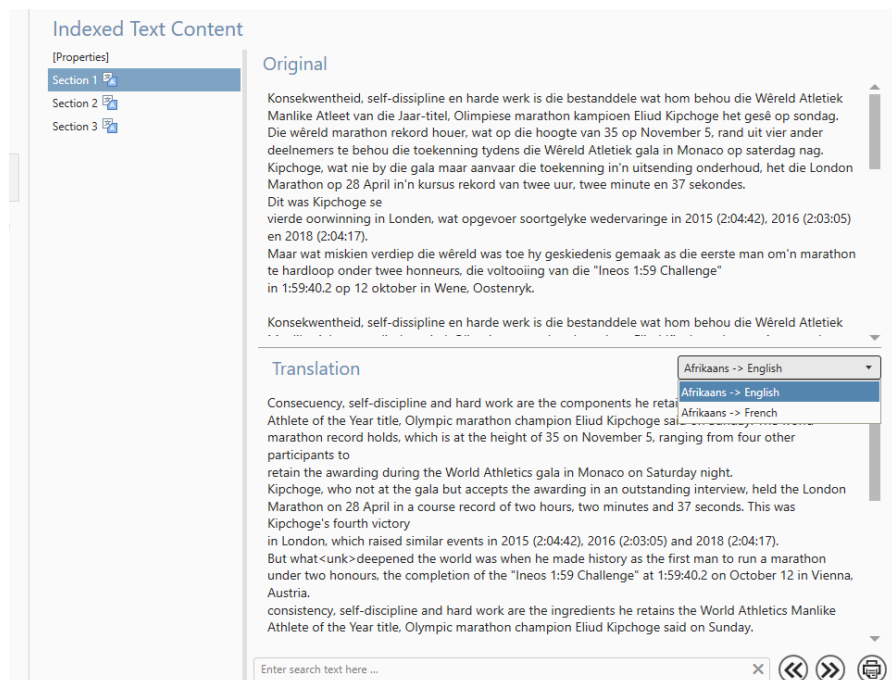
- Select START to run the job. This will take you to the JOBS tab and display the progress.

Figure 574



- Once the job has been completed, you can select VIEW RESULTS to view all the items in the EVIDENCE BROWSER.
- The results will be shown within the Text Index tab of the item's Omniviewer. It will display the Detego Offline Text Translator tag next to the document section (an A with a symbol next to it). The results will show the original text on top and the translation on the bottom.
- A new drop-down selector box is available in the text index view to switch between translations.

Figure 575



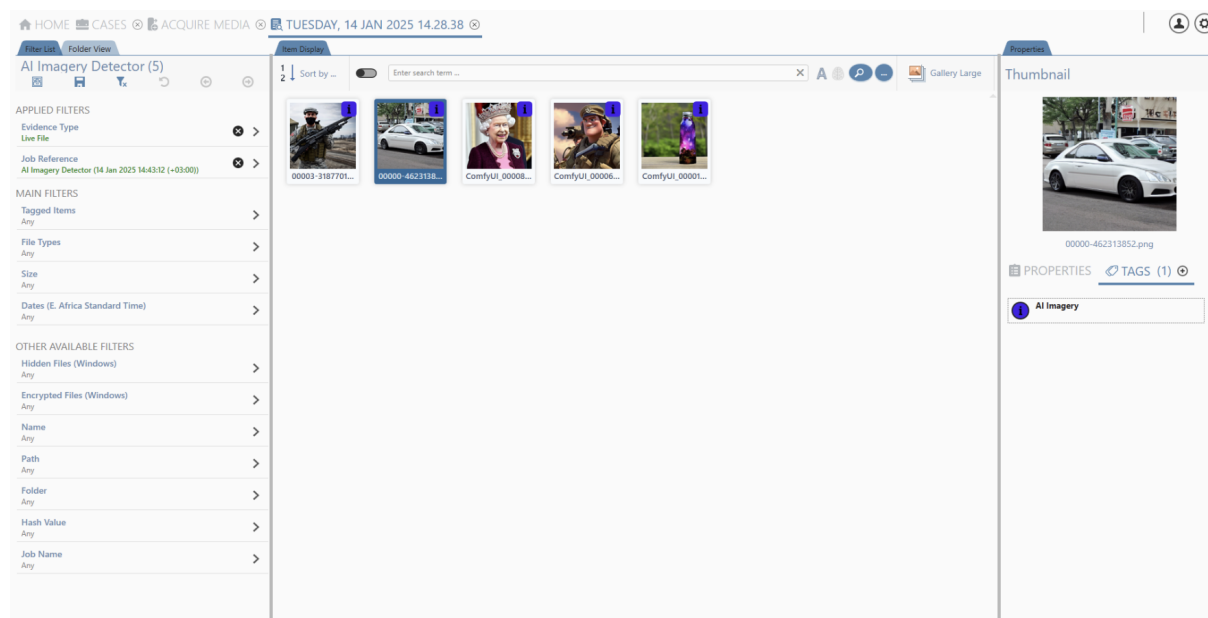
NOTE: A GPU is highly recommended for this analytic which forms part of the Detego Analyse AI+ suite of tools.

AI GENERATED IMAGE DETECTOR

Analyses the metadata of video and image evidence types to determine if the evidence item was AI generated.

The job applies **AI Imagery** tag to evidence items positively identified to be AI generated.

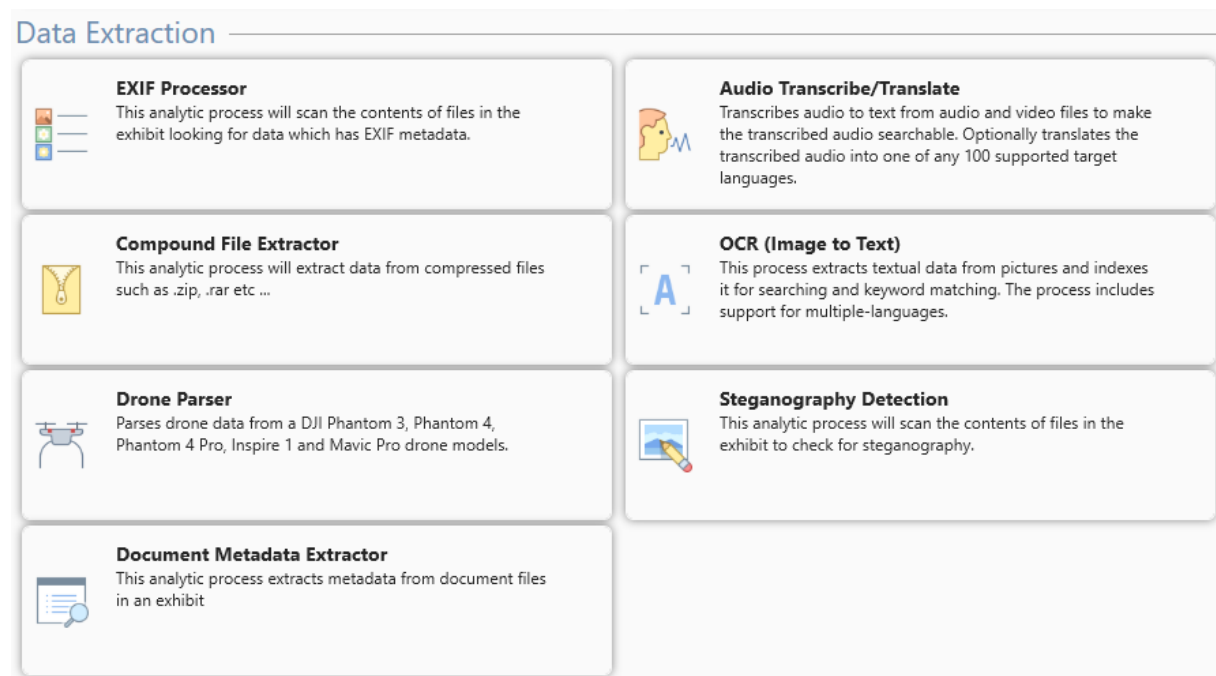
Figure 576



6.13. DATA EXTRACTION ANALYTICS

The Data Extraction Analytics extract further data from items.

Figure 577



EXIF PROCESSOR

EXIF ('Exchangeable Image File') metadata is embedded in image files created by any camera (including mobiles and smartphones) and provides a wealth of information to the examiner. Information like camera data, original image capture time, phone model, operating system, geographic location (longitude & latitude), and much more can typically be retrieved.

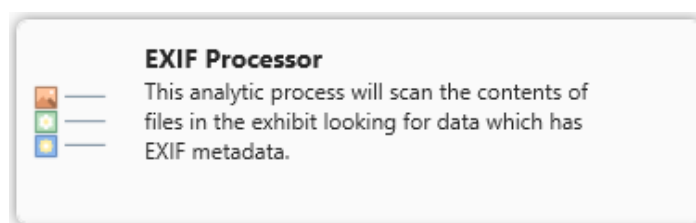
The EXIF Processor scans the content of an exhibit file to identify any of this metadata and displays this data in the Omniviewer. The data can be indexed using the 'Text Indexer' and matched against keywords.

Access to this intelligence may be the missing link placing a suspect at the crime scene.

To run the 'EXIF Processor', follow these steps:

- Open the 'Analyse and Manage' module and select the exhibit you wish to scan.
- Click on the 'Analytics' button along the bottom bar, OR right-click on the exhibit and select 'New Analytic' from the dropdown.
- From the 'Data Extraction' title, select the 'EXIF Processor' button to highlight it; a green tick will appear on the right.

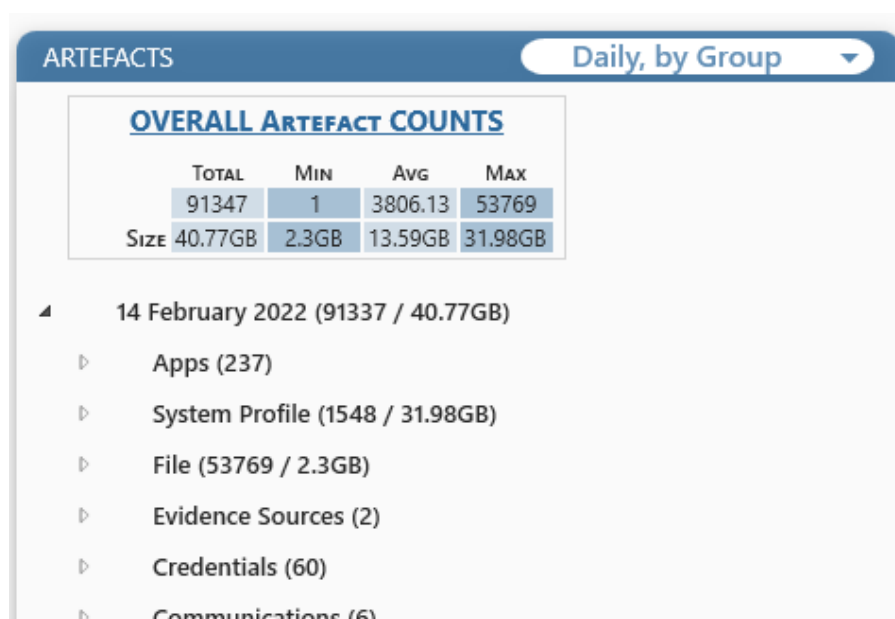
Figure 578



- Click on the 'START' button at the bottom of the pop-up. The process should run until completion with the results in the 'Jobs' tab.

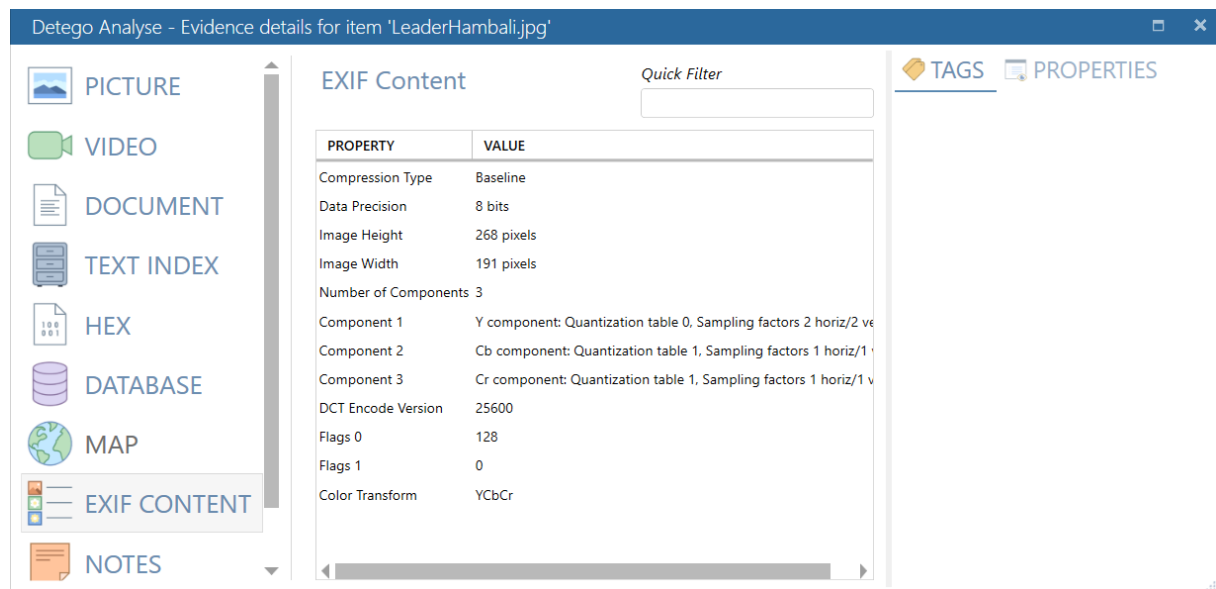
A summary of the extracted EXIF data is visible in the 'Metrics' tab under the 'ARTEFACTS' title.

Figure 579



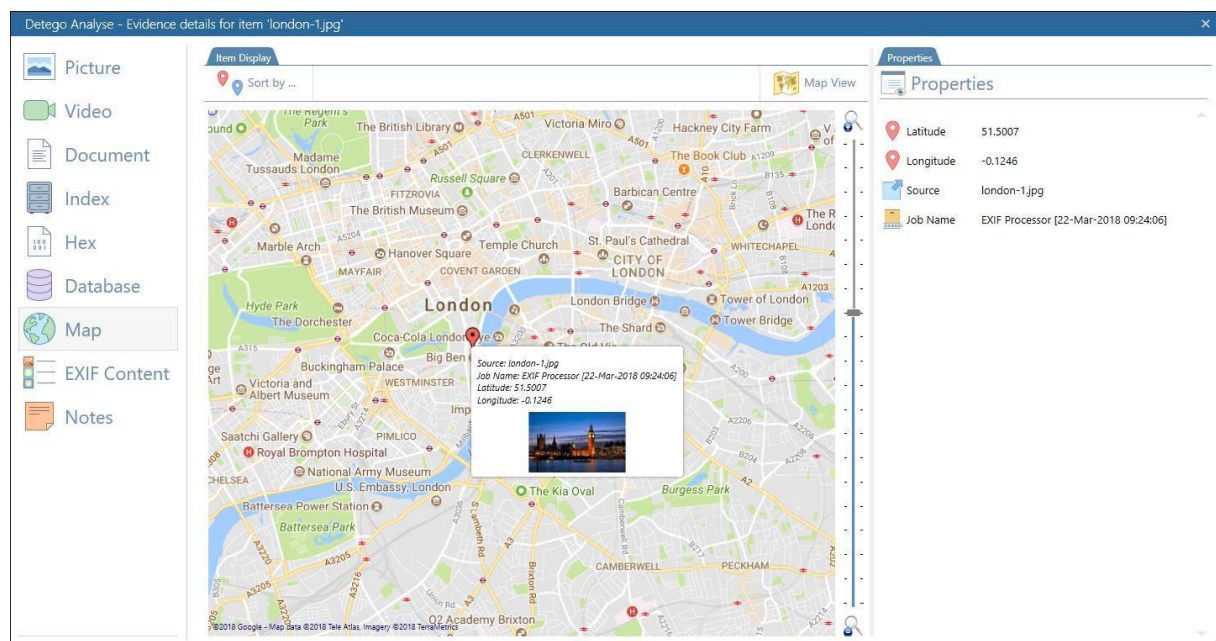
To view the EXIF data for a file, click on the 'Files' button in the 'Exhibit Content' tab and double-click the item you would like displayed. Click 'EXIF Content' from the menu on the left of the omniviewer.

Figure 580



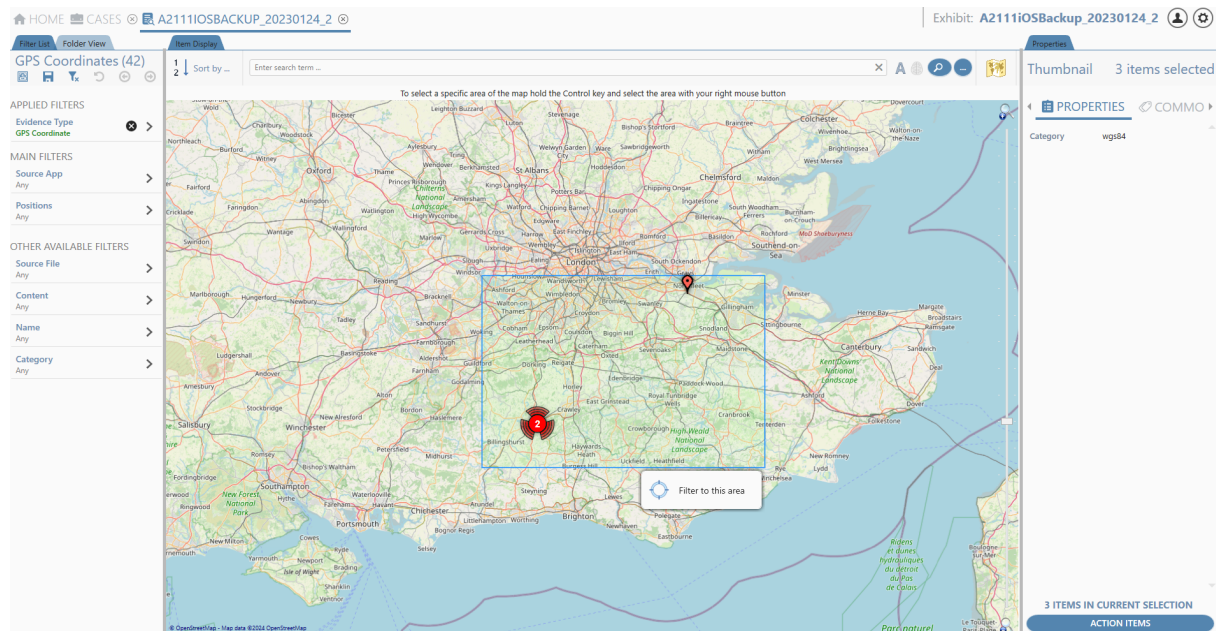
GPS data can also be viewed in the omniviewer by clicking 'Map' from the menu on the left.

Figure 581



Within the map view, you can also filter to a selected area by holding CTRL and Right Clicking around the area of the map you wish to filter to.

Figure 582



AUDIO TRANSCRIBE/TRANSLATE

A new analytic is available that will transcribe spoken audio and (in the case of non-English audio) translate the spoken audio. The transcribed/translated text is stored as a text index against the file, which can be searched using standard text search and keyword matching. The analytic can process audio from audio-only files and video files containing audio.

Figure 583

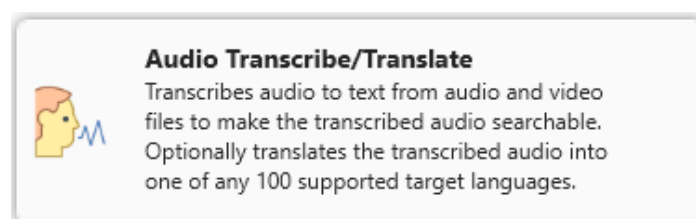


Figure 584

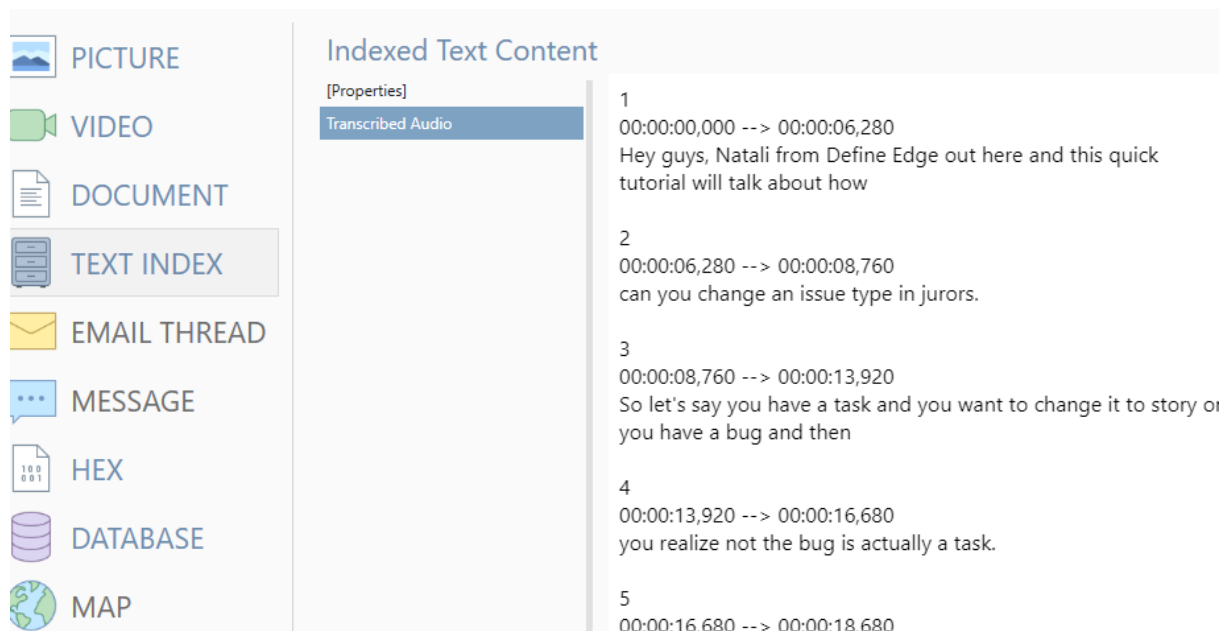
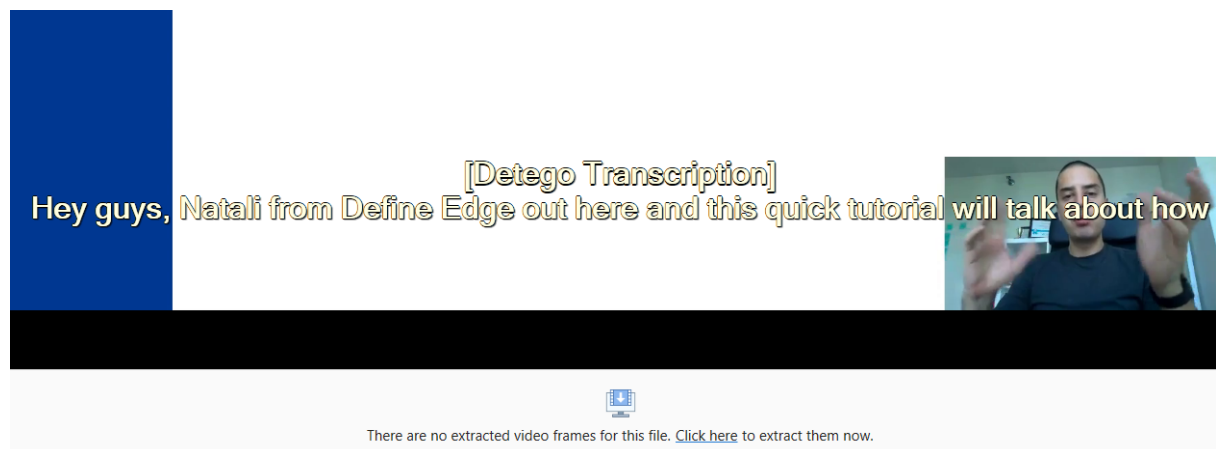
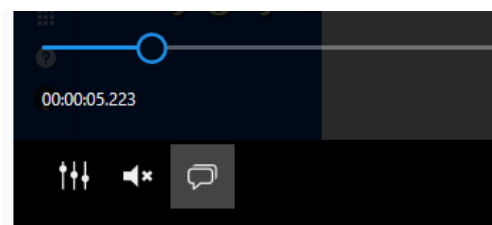


Figure 585



The indexed audio can be viewed in real-time as subtitles in the Detego video/audio viewer. These Detego-generated subtitles can be disabled using the player control (chat bubble icon).

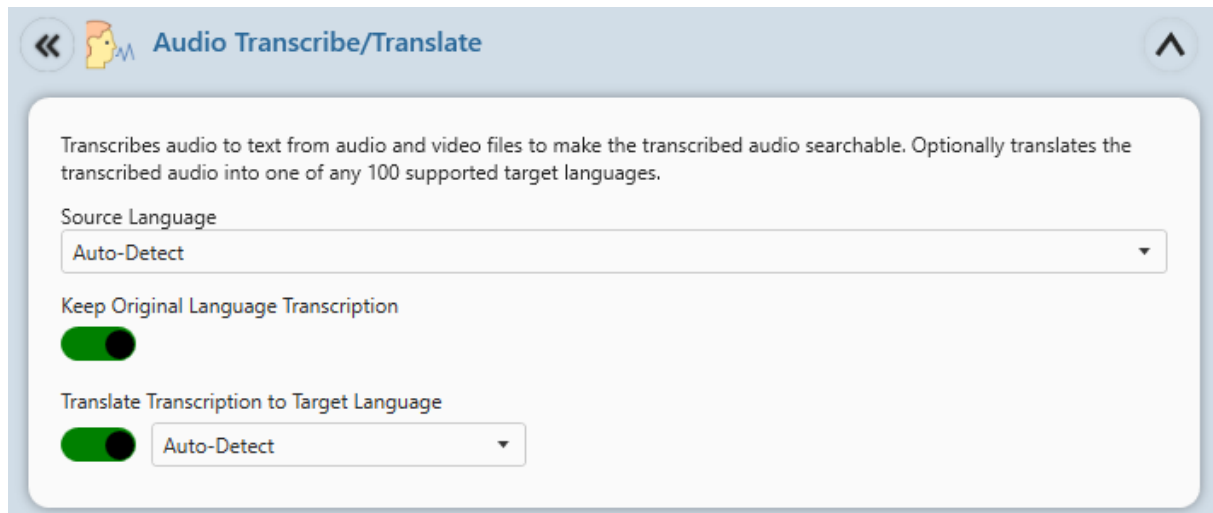
Figure 586



This supports keeping the transcription from the native spoken language as well as the translated copy. Translations can now be made to one of any 100 languages instead of just English compared to previous versions.

It is also now possible to manually select the source language to override the auto-detection if the spoken language of the audio is pre-known.

Figure 587



A GPU is highly recommended for this analytic which forms part of the Detego Analyse AI+ suite of tools.

COMPOUND FILE EXTRACTOR

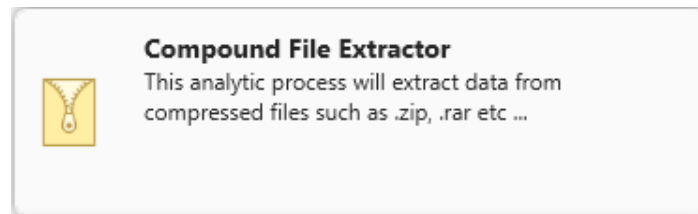
To reduce the time spent trying to access all the exhibits available to an examiner, the Compound File Extractor extracts data from compressed files, such as .rar, .tar, .zip, .VHD, .VHDX and .VMDK. It adds the extracted files to the exhibit for further analysis. You can also extract all files, individual archives, or only files less than a certain size. This also enables the ability to extract media from documents.

To extract all files at once, follow these steps:

- Open the 'Analyse and Manage' module and select the exhibit you wish to extract.
- Click on the 'Analytics' button along the bottom bar, OR right-click on the exhibit and select 'New Analytic' from the dropdown.

- Under the 'Data Extraction' title, select the 'Compound File Extractor' button to highlight it; a green tick will appear on the right. Please note that this method extracts data from all compressed files at once.

Figure 588



- Click on the 'START' button at the bottom of the pop-up.
- The extraction should run until completion with the results in the 'Jobs' tab.
- After successful completion, the number of files extracted per archive file will be displayed in the 'Jobs' tab.

To extract files using the 'ADVANCED...' options, follow these steps:

- Open the 'Analyse and Manage' module and select the exhibit you wish to extract.
- Click on the 'Analytics' button along the bottom bar, OR right-click on the exhibit and select 'New Analytic' from the dropdown.
- Under the 'Data Extraction' title, select the 'Compound File Extractor' button to highlight it; a green tick will appear on the right.
- Click on the 'ADVANCED...' button for additional options. Under 'Data Extraction', add the 'Compound File Extractor' to the 'Queued Jobs' column by clicking the arrow icon.

Figure 589

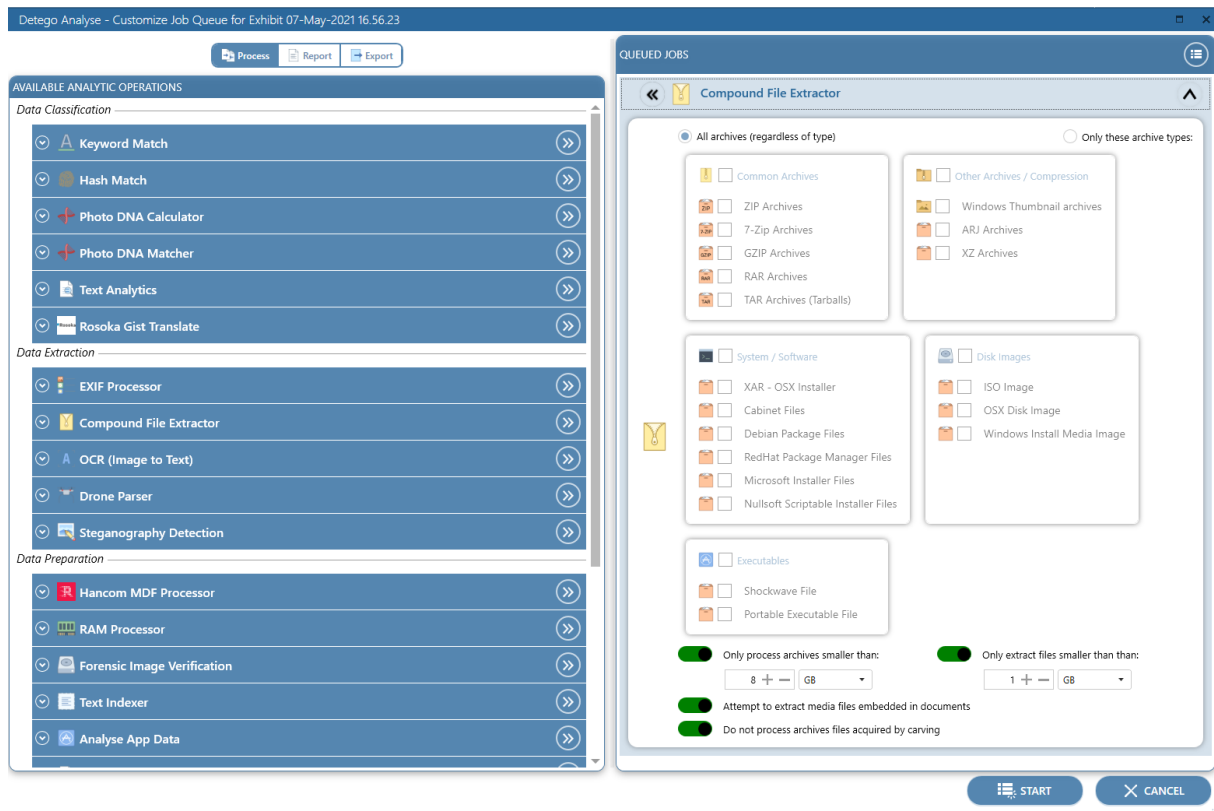
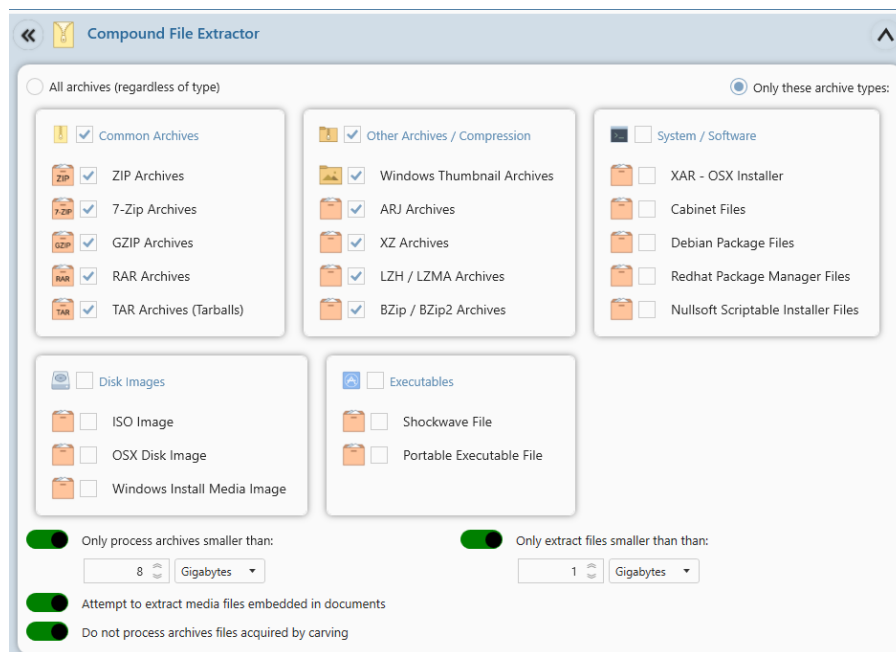


Figure 590



- Click on the 'START' button at the bottom of the pop-up. The extraction should run until completion. If successful, the number of files extracted per archive file will be indicated below in the 'Jobs' tab.

- The files extracted from the archives will now be visible within the exhibit content and available for analysis.

OCR (IMAGE TO TEXT)

OCR (Optical Character Recognition) technology normalises text in signs, number plates, written text and signatures into digital writing. The OCR analytical process extracts and indexes this textual data for searching and keyword matching.

To run the 'OCR', follow these steps:

- Open the 'Analyse and Manage' module and select the exhibit you wish to index. Click on the 'Analytics' button along the bottom bar, OR right-click on the exhibit and select 'New Analytic' from the dropdown.
- Select the 'OCR' button from the 'Data Preparation' title to highlight it; a green tick will appear on the right.

Figure 591

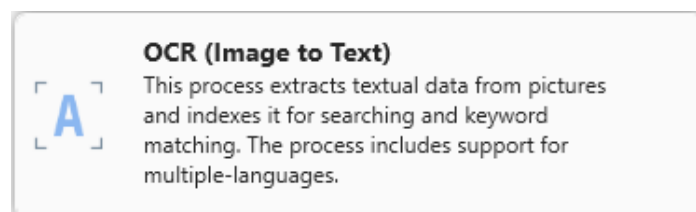
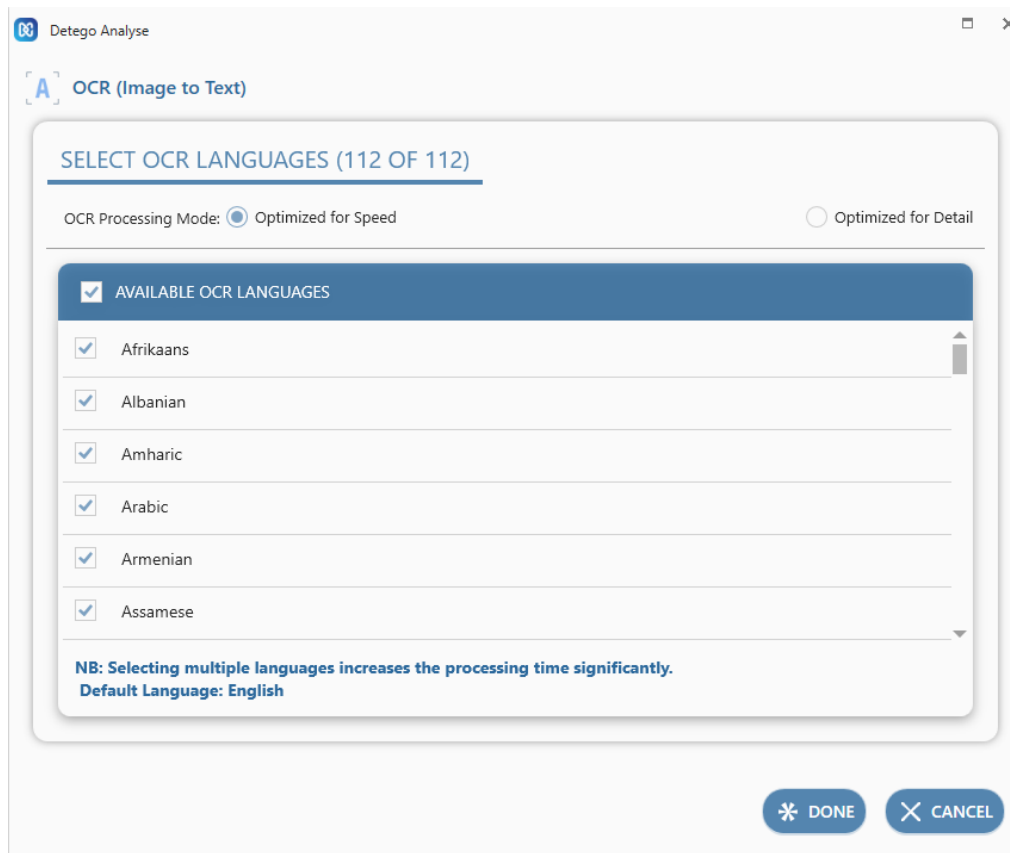


Figure 592



- You can choose between how OCR processing is Optimised for either:
 - Speed - This will perform faster but may not provide full results.
 - Detail - This may perform slower but will provide full results.
- Click on the 'START' button at the bottom of the pop-up. This will start the job and take you to the JOBS tab.
- Once the job is completed, you can select VIEW RESULTS to go straight to the EVIDENCE BROWSER to see the tagged items.

DRONE PARSER

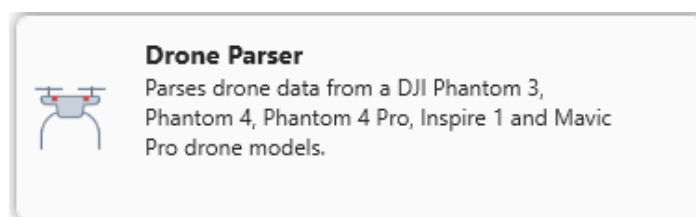
The 'Drone Parser' processes files from drones, such as the DJI Phantom III Standard, Advanced, Professional, and Inspire 1. The data parsed includes GPS locations, routes flown, altitude, acceleration, take-off, and landing points.

Note: The Media Acquisition module acquires a drone's SD card data.

To process files from drones, follow these steps:

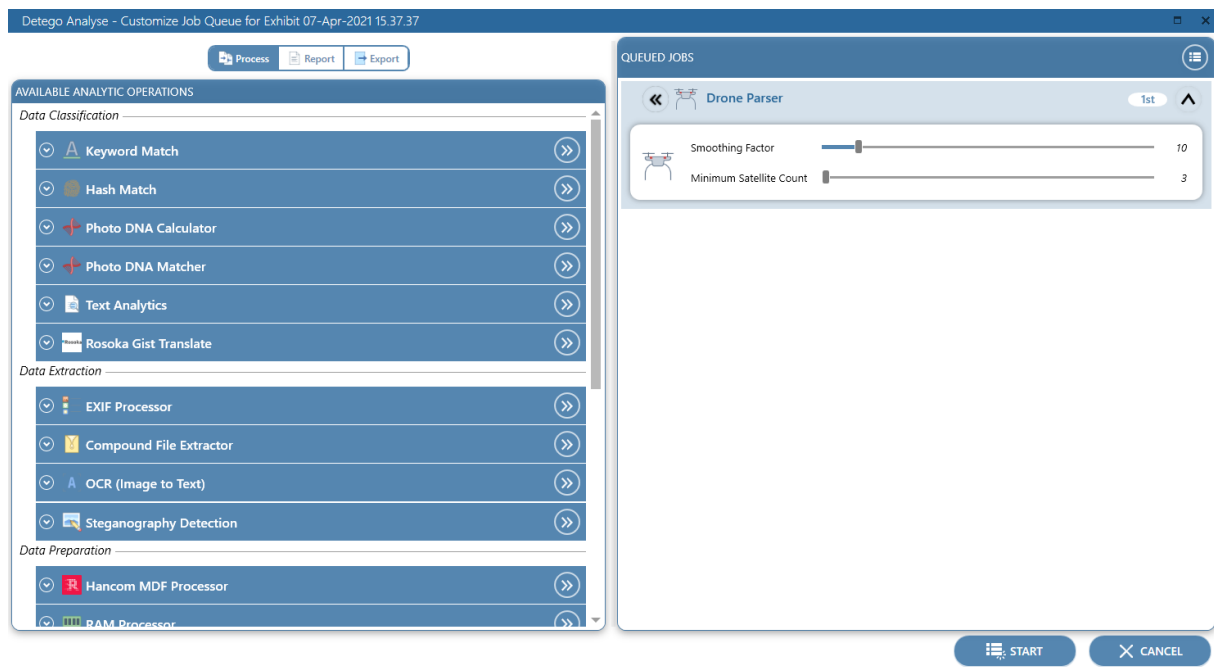
- Open the 'Analyse and Manage' module and select the exhibit you wish to process.
- Click on the 'Analytics' button along the bottom bar, OR right-click on the exhibit and select 'New Analytic' from the dropdown.
- From the 'Data Extraction' title, select the 'Drone Parser' button to highlight it; a green tick will appear on the right.

Figure 593



Click the 'START' button at the bottom of the window. This will start the job and take you to the JOBS tab.

Figure 594



- In the 'Analytics' window, you can select the Drone Parser job and select Advanced to open up the advanced options for the job.

This gives you two slider options.

- Smoothing Factor allows you to select the smoothing level applied to the flight data.
- Minimum Satellite Count – This allows you to select the minimum number of GPS satellites in view.
- Once you are ready, select START, and it will run the job.

The images below show the job running and after completion.

Figure 595

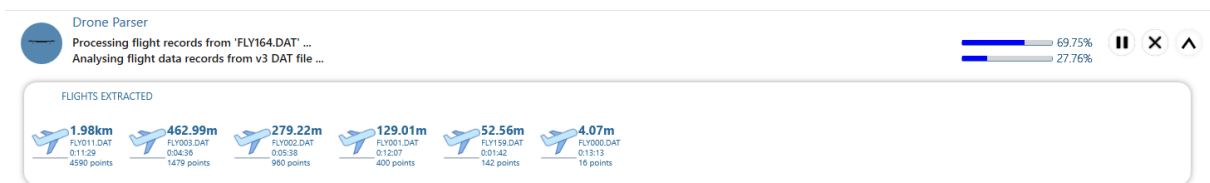
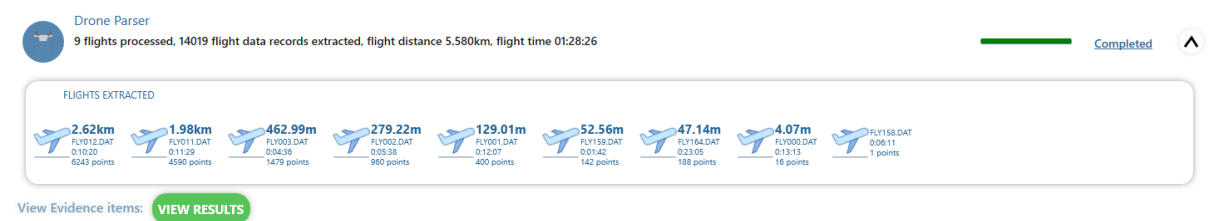


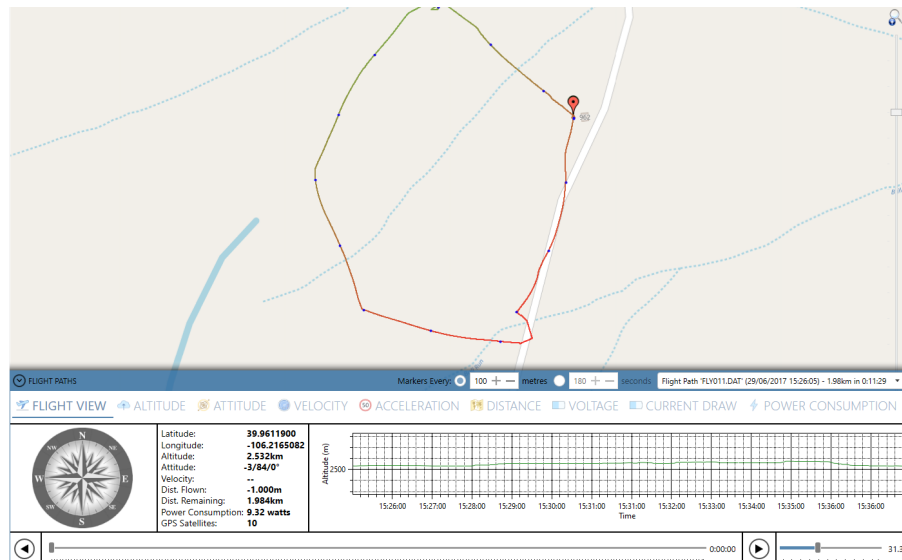
Figure 596



The operator can use the map to zoom into the different flight paths from the Evidence Browser. The path starts green, indicating take-off, and then becomes red until the point the drone lands. Clicking on any blue points opens a label containing additional information, including latitude, longitude, altitude and acceleration.

From the Flight Paths bar at the bottom of the window, you can select a specific flight path (right side of the bottom flight path panel dropdown).

Figure 597

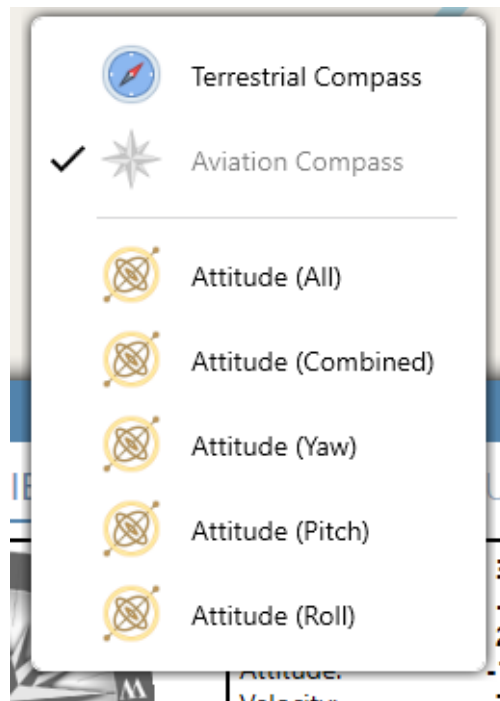


Once you have selected a flight path, you can open the Flight Path panel, and you will see the below tabs:

FLIGHT VIEW

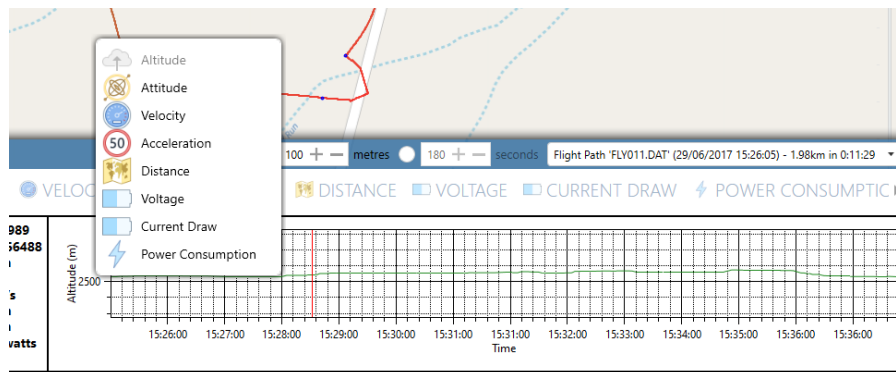
This shows you the flight View and allows you to check the various metrics during flight times. The left box displays an aviation compass by default but can be switched to a terrestrial compass by clicking it. It also allows you to select the drone's attitude during the flight, which includes Yaw, Pitch, Roll, Combined views and all views.

Figure 598



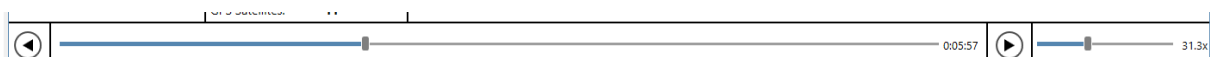
The box on the right side of the Flight Path panel displays a graph showing the altitude. This can be changed by right-clicking the pane and selecting the other options. This will change the graph to display that specific graph for the flight.

Figure 599



The bottom section of the panel displays a time scale with a button on either side. This time scale can be played forward or backward and dragged along to change the currently viewed time of the drone flight. The speed at which this plays can be determined by the right slider, allowing you to adjust the speed from 0.1x to 100x.

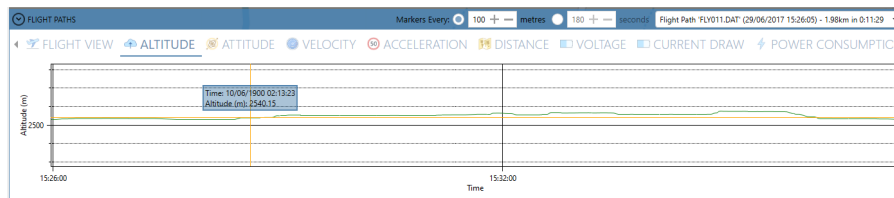
Figure 600



ALTITUDE

This tab displays a large-scale graph of the altitude of the flight path. Click and hold along the graph to see the exact altitude and time.

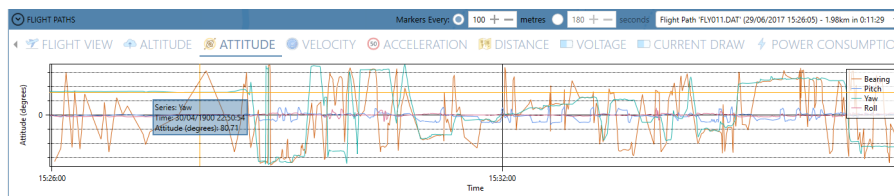
Figure 601



ATTITUDE

This tab displays a large-scale graph of the attitude of the flight path. There is a key on the right to explain which coloured line is Bearing, Pitch, Yaw and Roll. Selecting the line will give you attitude details for the point you clicked on.

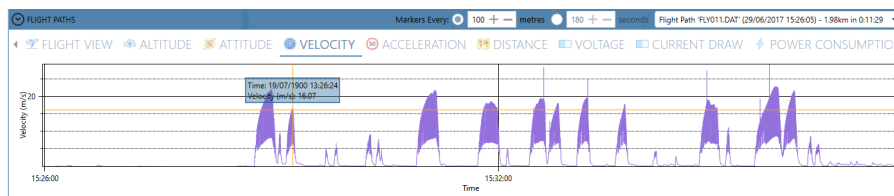
Figure 602



VELOCITY

This tab displays a large-scale graph of the velocity of the flight path. Clicking and holding will display the exact recorded velocity and time for that point in the flight.

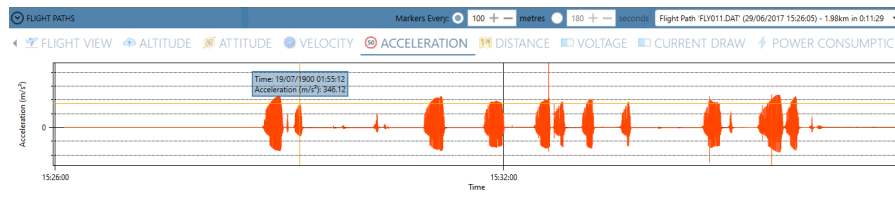
Figure 603



ACCELERATION

This tab displays a large-scale graph of the acceleration of the flight path. Clicking and holding will display the exact recorded acceleration and time for that point in the flight.

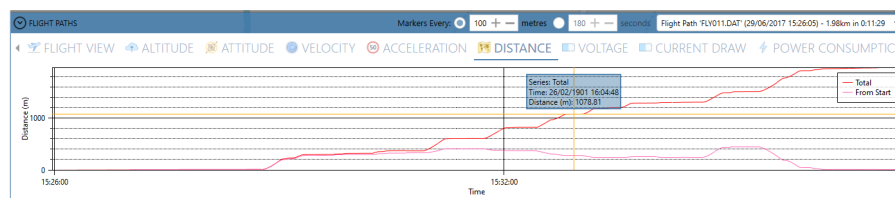
Figure 604



DISTANCE

This tab displays a large-scale graph of the distance of the flight path. The key on the right explains the coloured lines for 'Total' and 'From Start'. Clicking and holding will display the exact time and distance for the point selected.

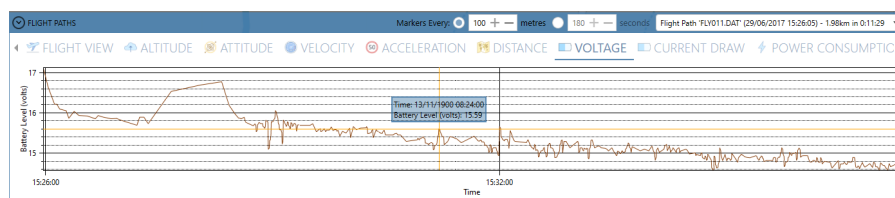
Figure 605



VOLTAGE

This tab displays a large-scale voltage graph during the flight path, determining battery level. Clicking and holding will display the exact battery level in volts and the time at the selected point.

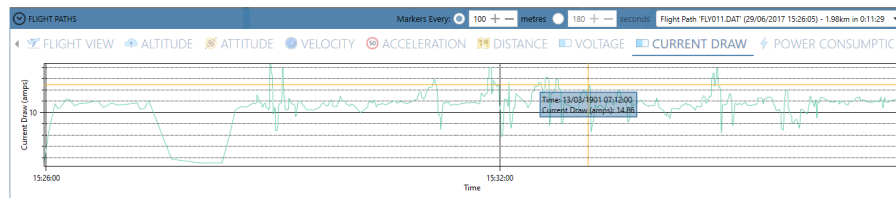
Figure 606



CURRENT DRAW

This tab displays a large-scale graph of the current draw during the flight path. Clicking and holding will display the exact current draw and the time of the selected point.

Figure 607



POWER CONSUMPTION

This tab displays a large-scale power consumption graph during the flight path. Clicking and holding will display the selected point's power consumption and time.

Figure 608

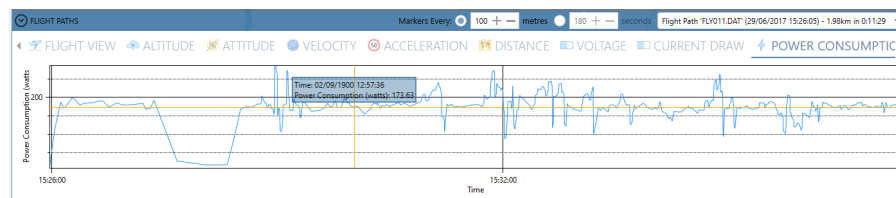
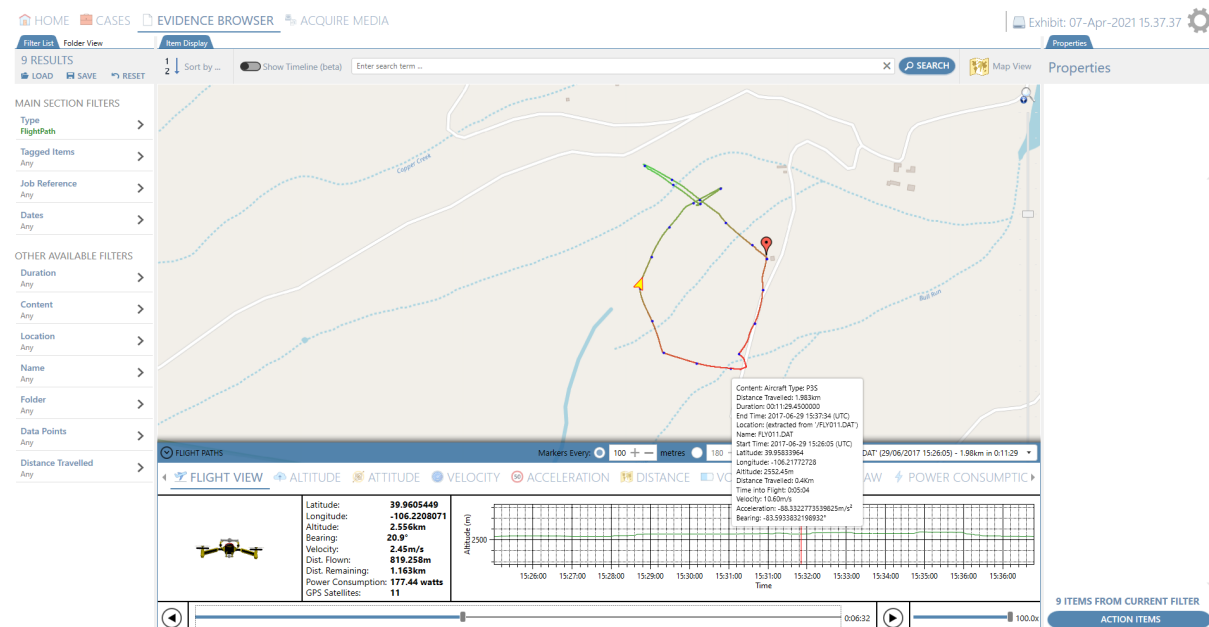


Figure 609



STEGANOGRAPHY DETECTION

Steganography hides information within a seemingly ordinary message so that only the intended recipient knows its existence. Although this art dates back more than 2,000 years, digital steganography works by replacing bits in files, such as images or audio, with private data so that criminals can send information undetected.

The 'Steganography Detection' process scans the contents of files in an exhibit, flagging files of interest for further analysis.

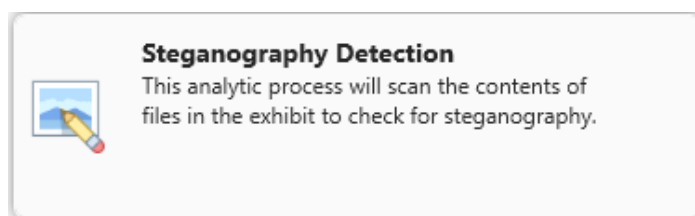
The Steganography job has been updated, so it will now find files injected inside MS Office document ZIP files. Files can be concealed in this way by opening the document as an archive and inserting files which should be hidden into them (after renaming the files as `.xml` files to avoid triggering Office file integrity detection).

The steganography detection job will now find such files, analyse the content to determine the correct type and extract them as evidence linked to the original document file.

To scan for steganography, follow these steps:

- Open the 'Analyse and Manage' module and select the exhibit you wish to search.
- Click on the 'Analytics' button along the bottom bar, OR right-click on the exhibit and select 'New Analytic' from the dropdown.
- Under the 'Data Extraction' title, select the 'Steganography Detection' button to highlight it; a green tick will appear on the right.

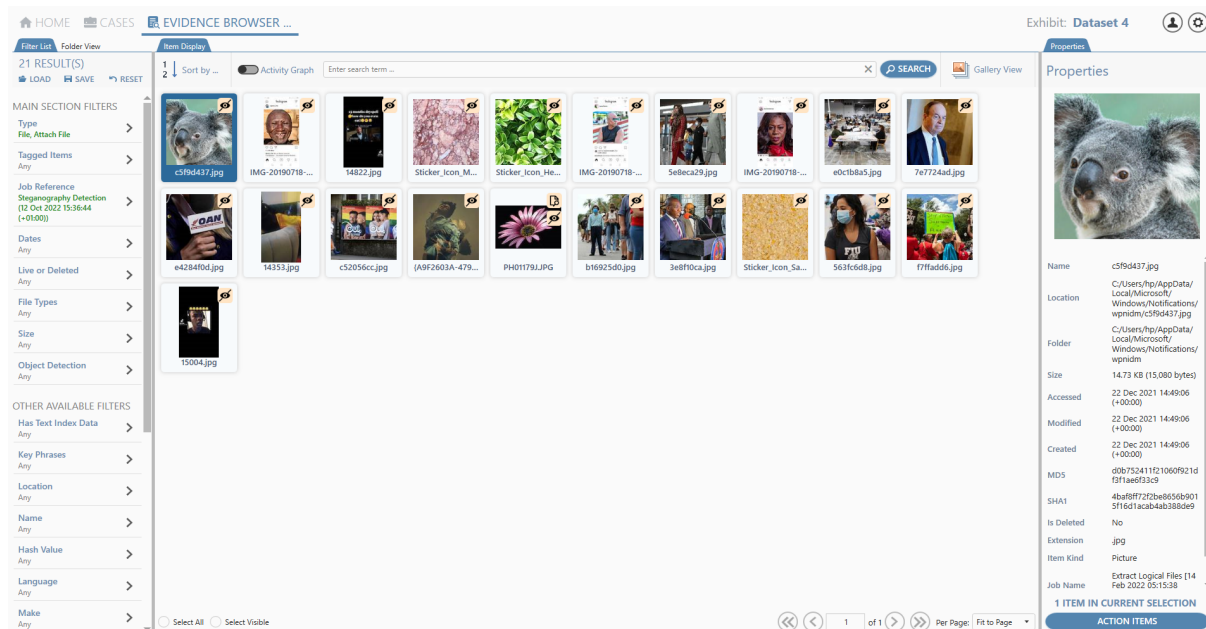
Figure 610



- Click on the 'START' button at the bottom of the pop-up. The extraction should run until completion; the image below appears on the 'Jobs' tab.

- The number of 'LOW', 'MEDIUM' and 'HIGH' steganography detections will be displayed, with flagged files appearing along the progress bar until the process has been completed.
- Files found to contain steganography are tagged and can be filtered from the rest of the exhibit data for further analysis by opening the 'Evidence Browser', toggling the 'Tagged Items' field and selecting 'Show all items which have selected tags'. From the 'System' dropdown, select only 'Steganography'.

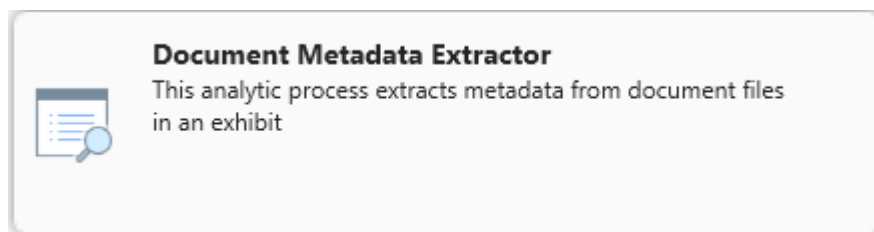
Figure 611



DOCUMENT METADATA EXTRACTOR

Document Metadata Extractor analytic job was added in Detego Analyse. This job extracts metadata from all document evidence types except plain text documents by default. The extracted metadata items are stored as indexed data, accessed through the Text Index tab of the omni viewer, under Document Metadata.

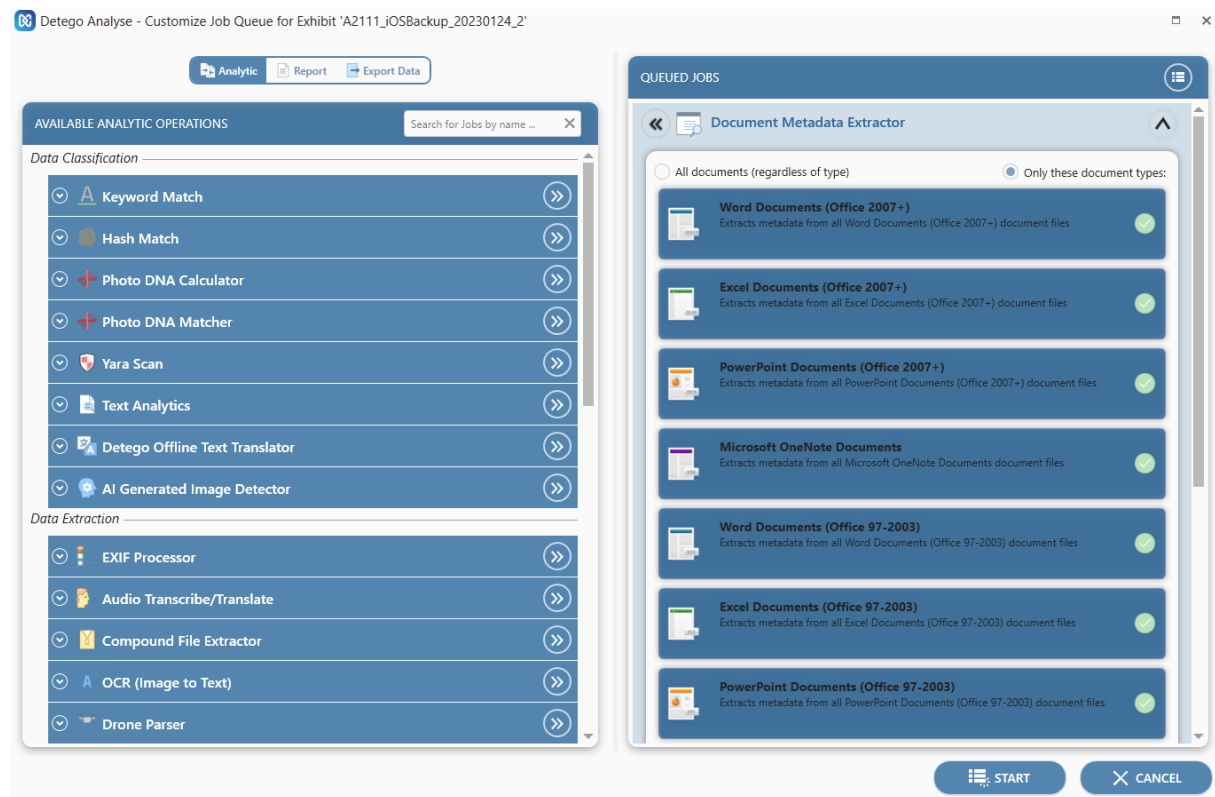
Figure 612



To run the analytic:

- Select the Document Metadata Extractor tile from within the Data Extraction Analytics section.
- Select START to run the analytic or ADVANCED if you wish to add other analytics or adjust what gets extracted.

Figure 613



- From the Advanced/Customize Job Queue window, you have the ability to select All documents regardless of type, or only document types of what is selected. It will default to selected only.
 - When you are ready, select START and it will begin the analytic.

Results:

Figure 614

Detego Analyse - Evidence details for item '8 (75).pdf'

Try New UI

INDEXED TEXT CONTENT

[Properties]

Document metadata

PDF Unmapped Unicode Chars Per Page : 0
 PDF Version : 1.5
 Xmp Creator Tool : Microsoft® Office Word 2007
 Contains XFA Forms : false
 Access Permission Modify Annotations : true
 X Tika Parsed By Full Set : org.apache.tika.parser.DefaultParser
 Dc Creator : Teach-Now
 Pdf Num 3 D Annotations : 0
 Created On : 2012-07-09T14:57:39Z
 Last Modified On : 2012-07-09T14:57:39Z
 Dc Format : application/pdf; version=1.5
 Pdf Docinfo Creator Tool : Microsoft® Office Word 2007
 Pdf Overall Percentage Unmapped Unicode Chars : 0.0
 Access Permission Fill in Form : true
 Pdf Docinfo Modified : 2012-07-09T14:57:39Z
 Pdf Has Collection : false
 Encrypted : false
 Pdf Contains Non Embedded Font : true
 Pdf Has Marked Content : true
 Pdf Ocr Page Count : 0
 File Type : application/pdf
 Access Permission Can Print Faithful : true
 PDF Creator : Teach-Now
 Dc Language : en-GB
 Pdf Producer : Microsoft® Office Word 2007
 Pdf Total Unmapped Unicode Chars : 0
 Access Permission Extract for Accessibility : true
 Access Permission Assemble Document : true
 Xmp T Pg N Pages : 1
 Contains XMP Metadata : false
 Pdf Chars Per Page : 2387
 Access Permission Extract Content : true
 Access Permission Can Print : true

Enter search text here ...

Match case?

PREVIOUS NEXT

PROPERTIES TAGS (1)

Name	8 (75).pdf
Location	/var/mobile/Applications/group.com.apple.FileProvider.LocalStorage/FileProvider Storage/Folder/8 (75).pdf
Folder	/var/mobile/Applications/group.com.apple.FileProvider.LocalStorage/FileProvider Storage/Folder
Size	164.62 KB (168,574 bytes)
Modified	08 Mar 2022 09:34:01 (UTC)
Created	08 Mar 2022 09:34:01 (UTC)
MDS	0e2649e596bc413ea894f186b3521284
SHA1	920affa8925c90f96fee21a6eb39d467b380c07
Application Source	Default
Extension	.pdf
Item Kind	Document
SHA256	f9d737cf22c5c5db9ac717f228cfc27d97b278c1b42849f7131a2a1df9eb0d0f

6.14. MEDIA PROCESSING ANALYTICS

The Media Processing Analytics section covers the various processing analytics for media including pictures and videos.

Figure 615

Media Processing

Video Frame Processor This analytic process will scan the contents of video files in the exhibit and produce frames at regular intervals.	Detego Visual Indexer Indexes the content of pictures to make their visual content searchable.
Picture & Video Analytics Processes pictures and videos for face, skin and object detection.	Indecent Images Detection Processes media for indecent images. Tags potential CSAM/IIOC material.
Symbols Detection Processes media for symbols detection e.g. symbols used by terrorist groups	Face Recognition Matches faces found in the exhibit against one or more face watchlists. Requires visual indexer to have been run beforehand.

VIDEO FRAME PROCESSOR

It's becoming increasingly common for criminals to hide secret messages inside video files, and whilst the untrained eye can't spot these subtle inconsistencies, the 'Video Frame Processor' can.

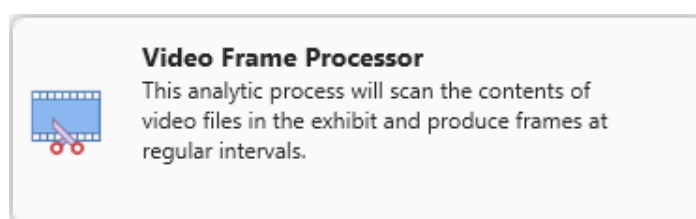
The Processor scans the content of an exhibit's video files, composing the visual content into still frames at specific predefined intervals (20, 30, 40 seconds, etc.). The captured frames are saved as .jpg files, with a naming convention of 'Frame001, Frame002... Frame010' and so on. These can then be searched for incriminating evidence through other analytical processes, such as the Text Indexer for OCR or the Picture and Video Analytics engine to detect different skin tones, faces and objects.

Please Note! This is one of the most resource-intensive tasks to run in Detego and is NOT recommended for use on minimum-spec machines.

To frame all the videos at once, follow these steps:

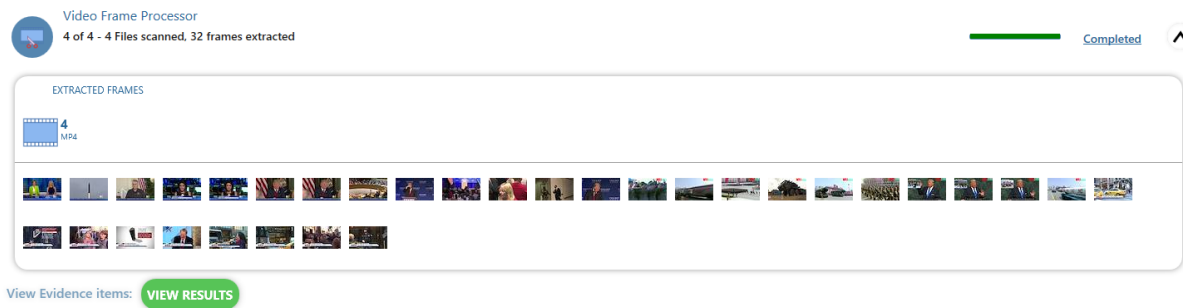
- Open the 'Analyse and Manage' module and select the exhibit you wish to scan.
- Click on the 'Analytics' button along the bottom bar, OR right-click on the exhibit and select 'New Analytic' from the drop-down.
- From the 'Media Processing' title, select the 'Video Frame Processor' button to highlight it; a green tick will appear on the right. Please note this will frame all the videos available in the exhibit.

Figure 616



- Clicking START will start the job and take you to the JOBS tab to view the progress.
- Once completed, you can select the VIEW RESULTS button, which will take you straight to the EVIDENCE BROWSER tab, where you can view the newly tagged items.

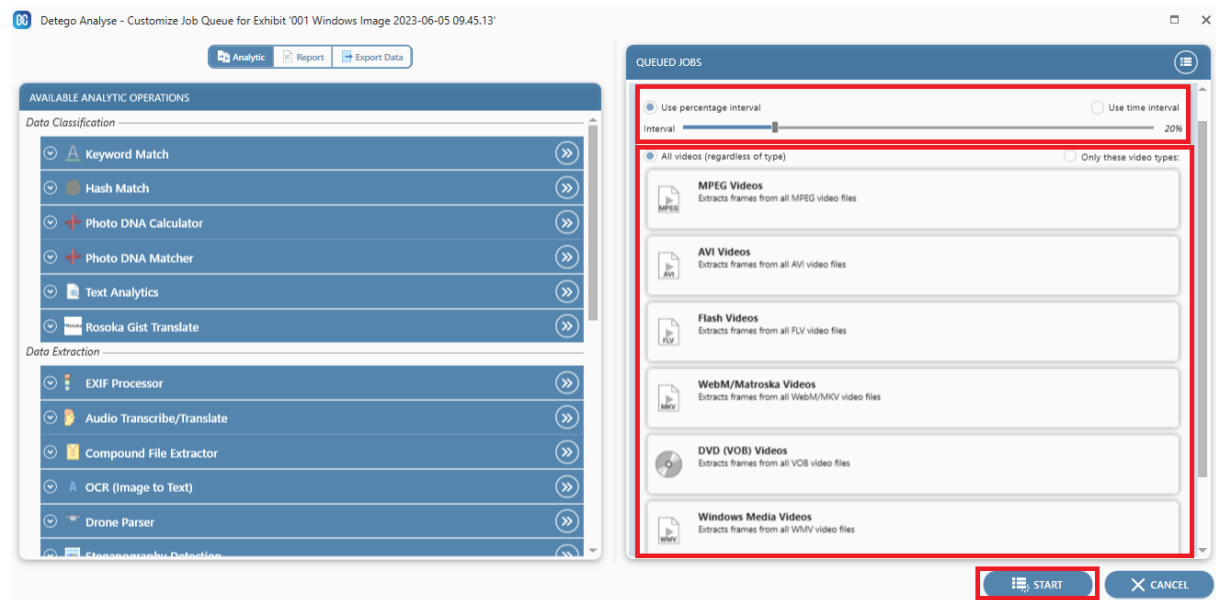
Figure 617



To frame files using the 'ADVANCED...' options, follow these steps:

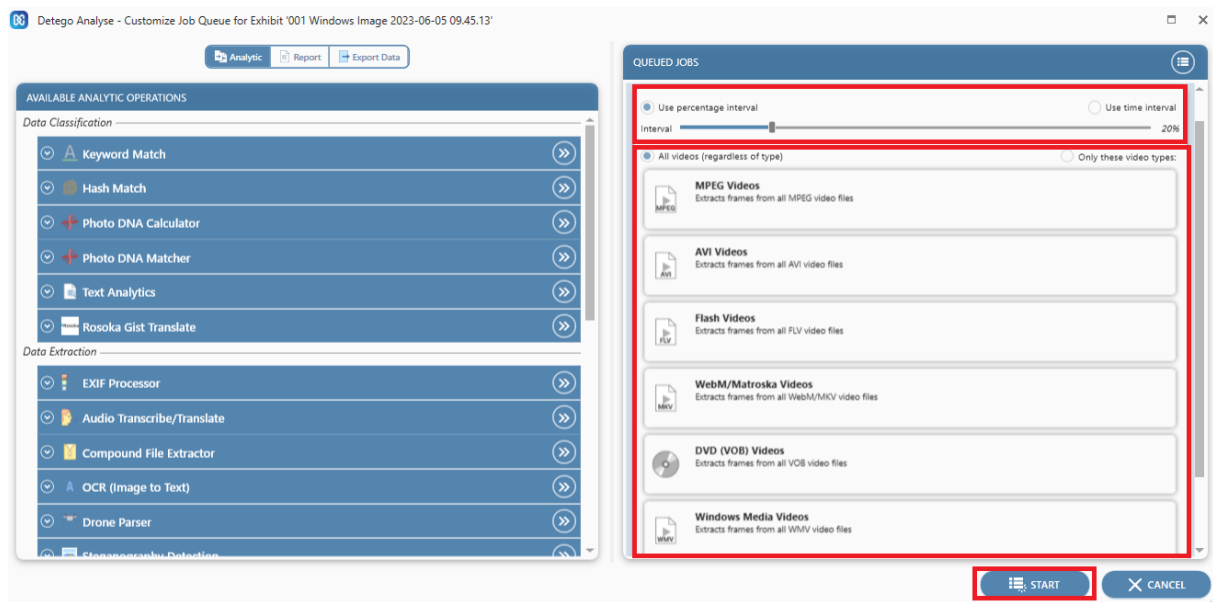
- Open the 'Analyse and Manage' module and select the exhibit you wish to scan.
- Click on the 'Analytics' button along the bottom bar, OR right-click on the exhibit and select 'New Analytic' from the drop-down. From the 'Media Processing' title, select the 'Video Frame Processor' button to highlight it; a green tick will appear on the right.
- Click on the 'ADVANCED...' button for additional options. Under 'Media Processing', add the 'Video Frame Processor' to the 'Queued Jobs' column by clicking the arrow icon.

Figure 618



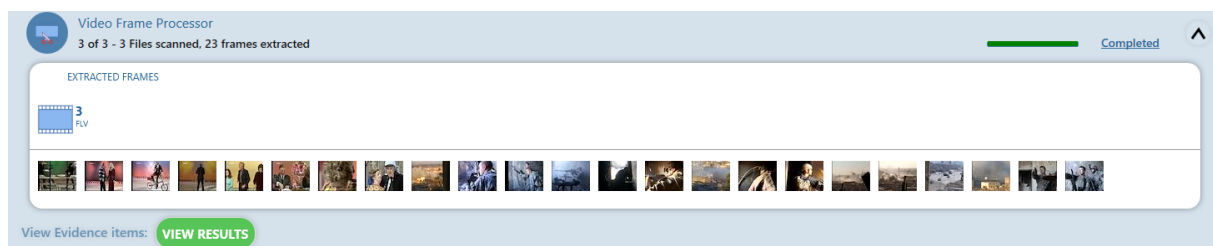
- To scan all files, use the default settings, ensuring the 'All videos (regardless of type)' radio button is selected. To choose specific files, click the 'Only these video types' and select which to scan from the list. The operator can also adjust the interval length (in percentage of total length) using the slider at the bottom of the pop-up.

Figure 619



- Click on the 'START' button at the bottom of the pop-up. The process should run until completion. The image below shows how it appears on the 'Jobs' tab, with the figures indicating the number of frames captured.

Figure 620



The default naming policy for video frames has been changed to `Frame #n` rather than the previous method of appending the second number to the frame name. The exact frame time is specified in a property of the video frame.

DETEGO VISUAL INDEXER

A new analytic, 'Detego Visual Indexer,' has been introduced. Once this job has been run on an exhibit, it will enable additional search functionality within the evidence browser.

Figure 621

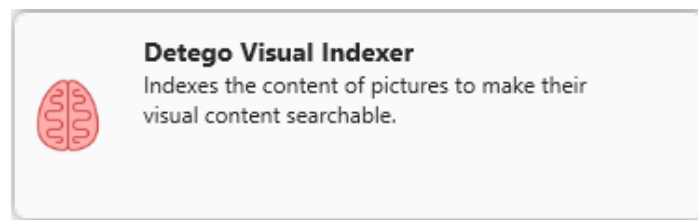
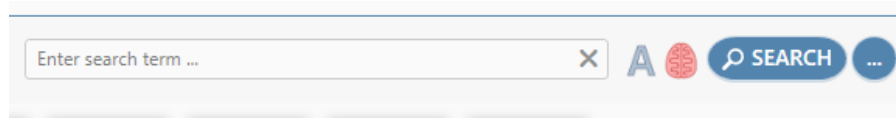


Figure 622



The new search controls allow text-to-image and image-to-image searching. The search is an approximate/similarity search.

Figure 623

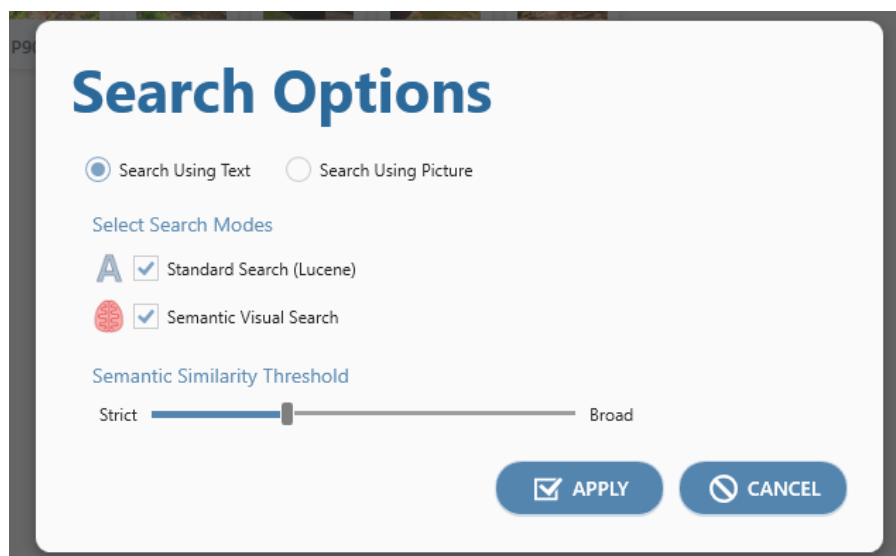
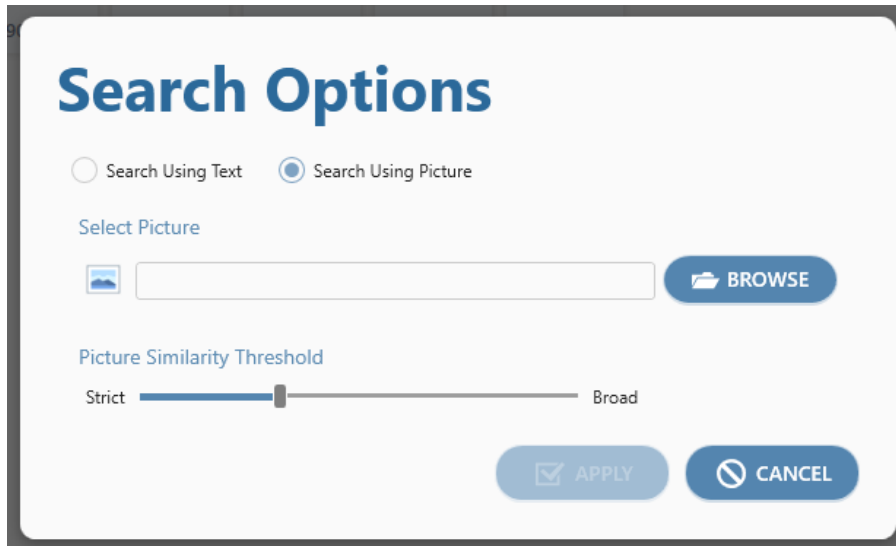
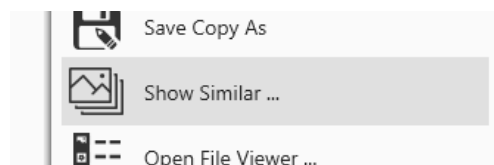


Figure 624

A dialog box titled "Search Options" in a large blue font. It contains two radio buttons: "Search Using Text" (unselected) and "Search Using Picture" (selected). Below this is a section labeled "Select Picture" with a small picture icon, a text input field, and a blue "BROWSE" button with a folder icon. Further down is a "Picture Similarity Threshold" section with a slider ranging from "Strict" to "Broad", with a blue bar indicating the current position. At the bottom are two buttons: "APPLY" (with a checkmark icon) and "CANCEL" (with a close icon).

For image-to-image search, the user can supply their image using the image-to-image search options. Alternatively, the user may select a picture file within the exhibit and right-click → 'Show Similar' to show other similar pictures within the exhibit.

Figure 625



The search results are sorted with the most similar matches appearing first in the evidence browser view. Semantic search picture matches are shown before any standard text search matches.

PICTURE & VIDEO ANALYTICS

The 'Picture & Video Analytics' engine is built to detect faces, skin and specific objects, significantly reducing the time investigators spend sifting through files and freeing them up to focus on other tasks.

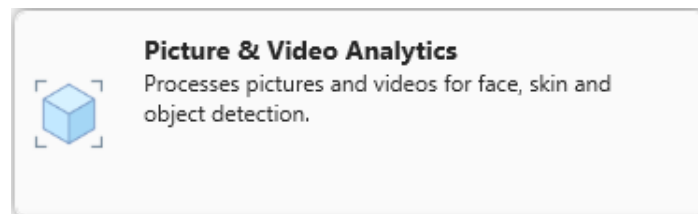
Once the initial analysis has been completed, the engine can be configured to drill down into the evidence. It can flag a specific face, detect different skin tones and even scan and identify predefined objects (including weapons, drugs, people and vehicles) that may be important to a case.

Face, skin and object matches are flagged in the 'Evidence Browser'.

To process images and videos using the default settings, follow these steps:

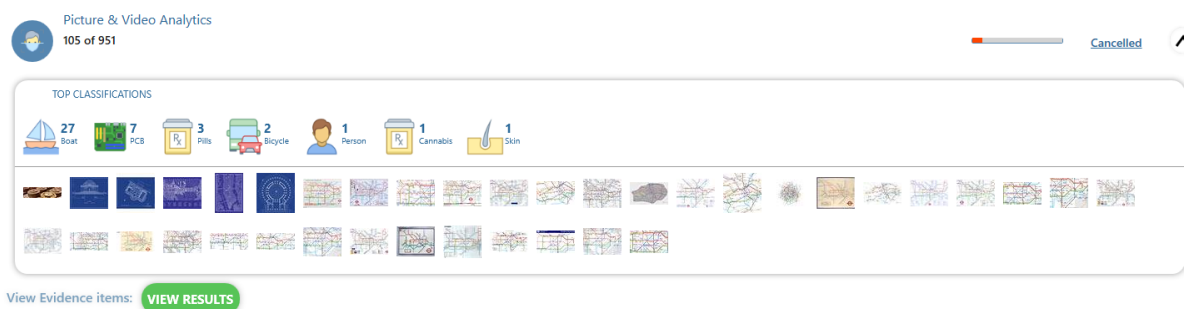
- Open the 'Analyse and Manage' module and select the exhibit you wish to scan.
- Click on the 'Analytics' button along the bottom bar, OR right-click on the exhibit and select 'New Analytic' from the drop-down.
- Select the 'Picture & Video Analytics' button from the 'Media Processing' title to highlight it; a green tick will appear on the right. Click the 'START' button at the bottom of the window.

Figure 626



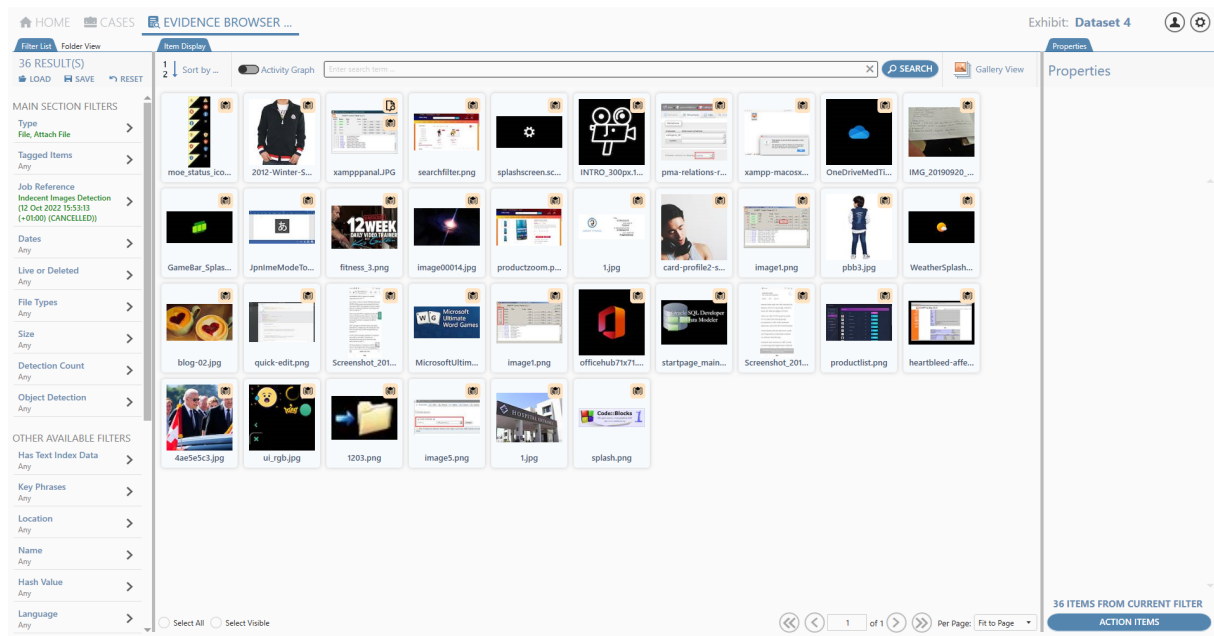
- The process should run until completion and automatically take you to the JOBS tab.

Figure 627



- Once the job has been completed, you can select VIEW RESULTS to go straight to the EVIDENCE BROWSER and view the items with their appropriate tags.

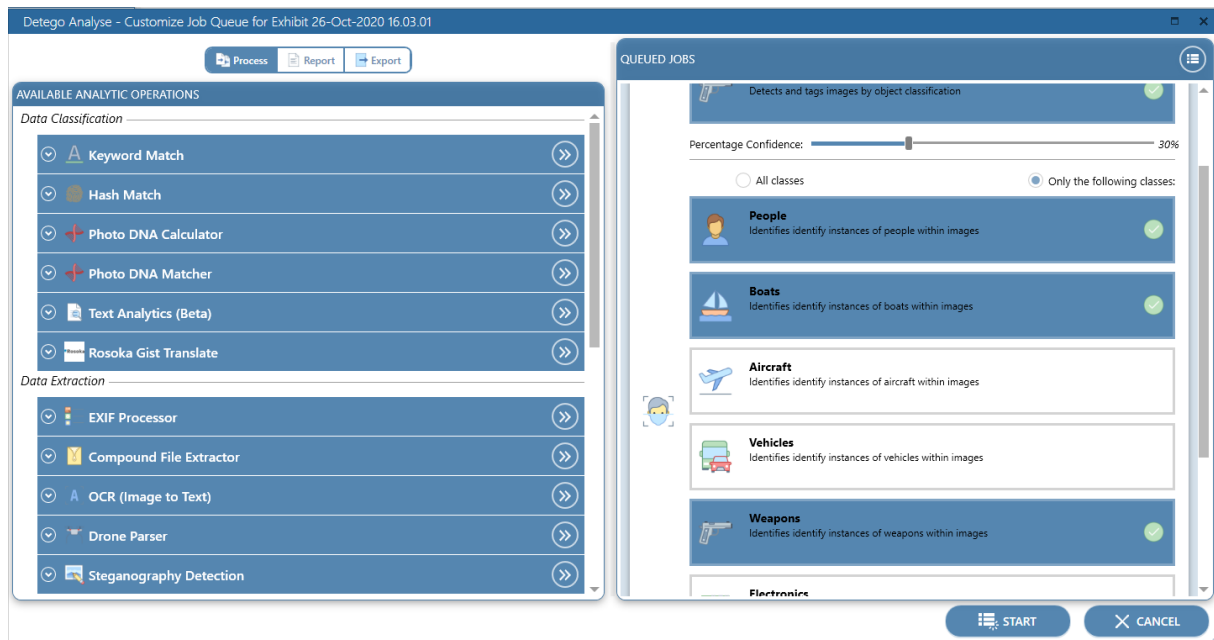
Figure 628



To process the images and videos using the advanced settings, follow these steps:

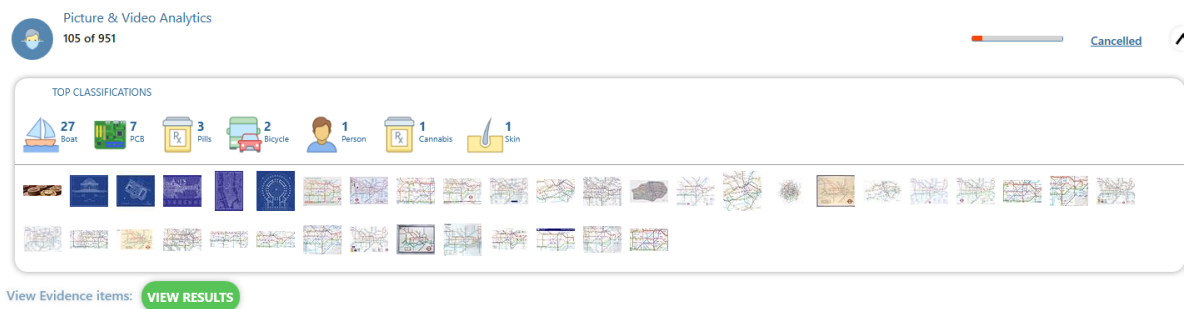
- Open the 'Analyse and Manage' module and select the exhibit you wish to scan.
- Click on the 'Analytics' button along the bottom bar, OR right-click on the exhibit and select 'New Analytic' from the drop-down.
- Select the 'Picture & Video Analytics' button from the 'Media Processing' title to highlight it; a green tick will appear on the right.
- Click on the 'ADVANCED...' button for additional options. Under 'Media Processing', add the 'Picture & Video Analytics' to the 'Queued Jobs' column by clicking the arrow icon.

Figure 629



The process should run until completion; the image below shows how the results are displayed in the 'Jobs' tab with the figures and icons indicating the number of faces, the percentage of skin tones and which objects were detected.

Figure 630



INDECENT IMAGES DETECTION

The Indecent Image Detection Analytic engine is built to detect Child Sexual Abusive Material, Indecent Images of Children and other material of a sexually explicit nature.

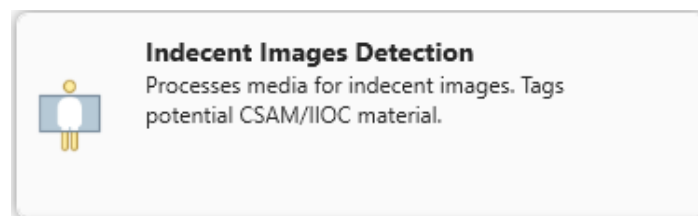
The analytic engine is ideal for detecting first-generation images and victim identification.

The job processes media for indecent images and tags potential CSAM/IIOC material. It is a preconfigured job with no customisation options.

To run the job, follow the below steps:

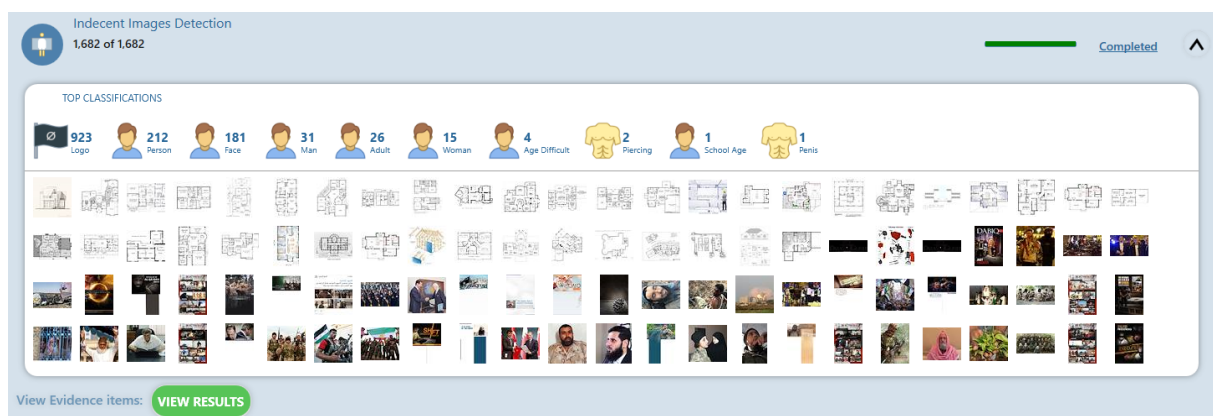
- Select the exhibit you wish to run the 'Indecent Images Detection' job from the 'Analyse and Manage' tile in the CASES window.
- Select the 'Analytics' button at the bottom of the window OR right-click the exhibit on the left panel and select 'New Analytic'.
- Select the 'Indecent Images Detection' job from the Analytics window and select START to run the job.

Figure 631



- When you click START, the job will commence, and you will be taken to the JOBS tab.
- Once the job is complete, you can select VIEW RESULTS, which will take you straight to the EVIDENCE BROWSER to view the tagged items.

Figure 632



SYMBOLS DETECTION

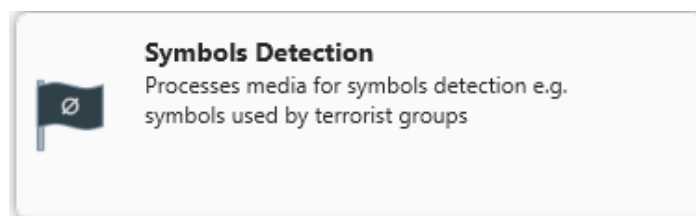
The Symbol Detection job is similar to Picture and Video Analytics. It processes media for symbols used by terrorist groups.

Unlike Picture & Video Analytics, the Symbols Detection job is preconfigured without customisation.

To run the Symbols Detection job, follow the below steps:

- Open the 'Analyse and Manage' module and select the exhibit on which you wish to run the job.
- Click the 'Analytics' button at the bottom of the window OR right-click the exhibit on the left panel and select 'New Analytic'.
- Select the 'Symbols Detection' job from the Analytics window under the 'Media Processing' section and select START.

Figure 633



- Clicking START will start the job and take you to the JOBS tab to view the progress.
- Once completed, you can select VIEW RESULTS to take you straight to the EVIDENCE BROWSER with the items that will now be tagged with symbols detected.

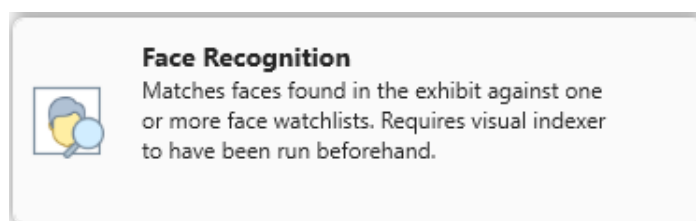
Figure 634



FACE RECOGNITION

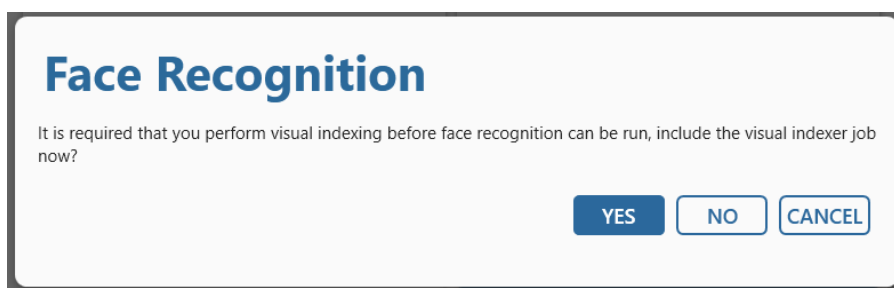
To run the face recognition, select the exhibit that should be searched. Select the 'Detego Visual Indexer' and 'Face Recognition' analytic jobs. The face recognition job will prompt you to select the face watchlist to run against the exhibit.

Figure 635



If you do not select the visual indexer, a warning will be displayed.

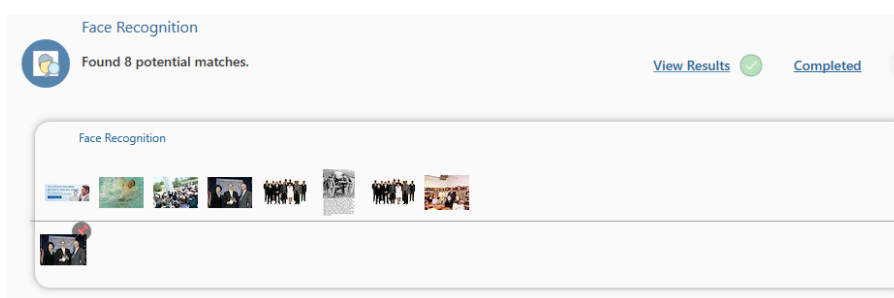
Figure 636



Viewing Results

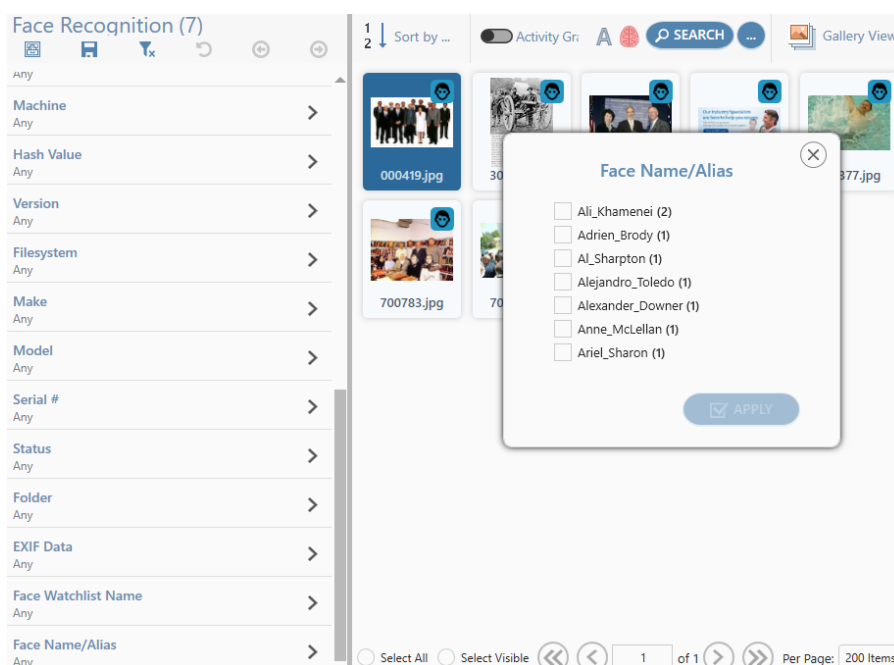
When the job runs, potential matches will be displayed as it progresses. When the job has been completed, click the 'View Results' link to view the filtered results in the evidence browser.

Figure 637



Filters are then available for 'Face Watchlist Name' and 'Face Name/Alias'. Files matched against a face watchlist have a blue face tag.

Figure 638



6.15. PASSWORD PROCESSING ANALYTICS

Note: The functionality to detect and unlock encrypted files is a 'paid for' add-on within the Detego Unified Forensics Platform. If you cannot access it, please contact your account manager at marketing@detegoglobal.com.

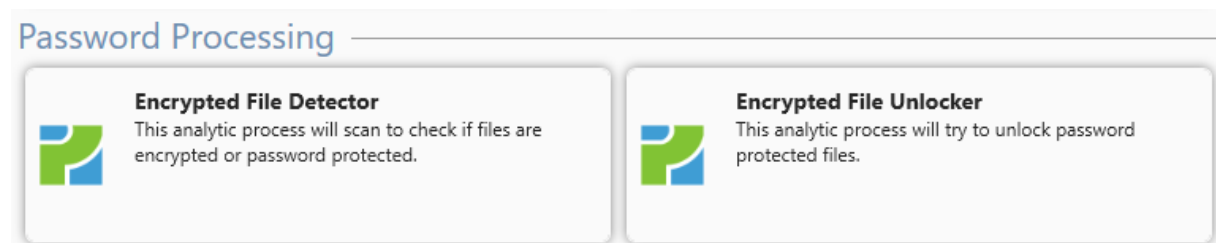
Password-protected containers are undoubtedly there for a good reason, but they also often hold the most pertinent information regarding an investigation.

Password recovery technology Passware has partnered with MCM Solutions to integrate their industry-leading solution into the Detego Unified Forensics Platform, allowing users to identify encrypted evidence and seamlessly recover breakthrough passwords from over 250 file types (including MS Office, PDF, ZIP & RAW, and FileMaker), all from one platform.

Not only does our Encrypted File Detector and Unlocker automatically identify every encrypted and password-protected folder on a device, but it can also effortlessly launch a series of attacks to break through and gain access.

This tool recovers passwords from computers, Apple iPhone/iPad, Android backups, and Android images.

Figure 639



Please make sure you have followed the installation guide to install Passware correctly.

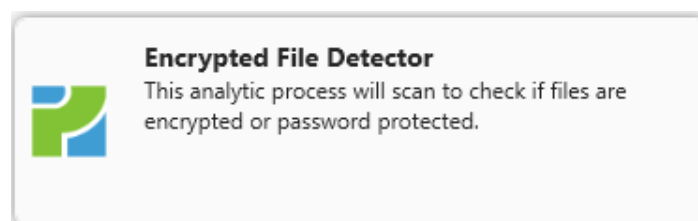
ENCRYPTED FILE DETECTOR

The 'Encrypted File Detector' scans extracted files and disk images, reporting encryption types and decryption complexity and flagging password-protected ones for further analysis.

Follow the below steps to run the Encrypted File Detector job:

- Select your exhibit from the Analyse and Manage module on the left panel.
- Select the 'Analytics' button at the bottom of the window OR right-click the exhibit on the left panel and select 'New Analytic'.
- Scroll to the 'Password Processing' section from the Analytics window and select 'Encrypted File Detector'.

Figure 640



- Select START to run the job; this will also take you to the JOBS tab to view the progress.
- From the JOBS tab, you can see the number of files scanned and the number of files in the exhibit. You can also select VIEW RESULTS, which will take you to the EVIDENCE BROWSER to see the items discovered.

Figure 641

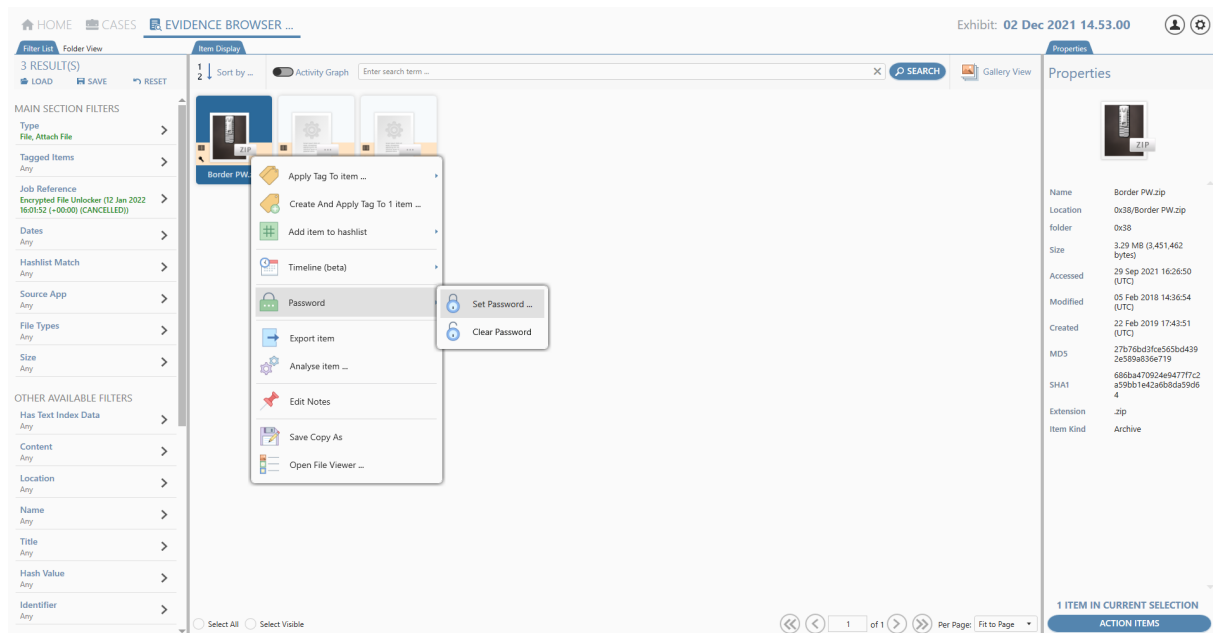


ENCRYPTED FILE UNLOCKER

Once the 'Encrypted File Detector' process has found encoded files, the 'Encrypted File Unlocker' process attempts to find passwords for the encrypted files and unlock them.

If you already know the password for an encrypted folder after detecting it with Password Detector, you can right-click the item, select Password and 'Set Password.' This allows you to open and unlock the folder without using Password Unlocker, which can take some time.

Figure 642



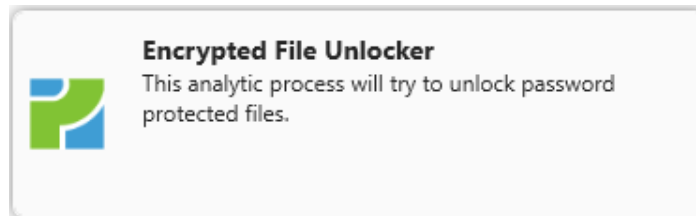
Running 'Compound File Extractor' is recommended after successfully unlocking the encrypted folder.

To run the 'Encrypted File Unlocker' job, follow the below steps:

- Select the exhibit you wish to run the process on from the 'Analyse and Manage' module.
- Select the 'Analytics' button at the bottom of the window OR right-click the exhibit on the left panel and select 'New Analytic'.

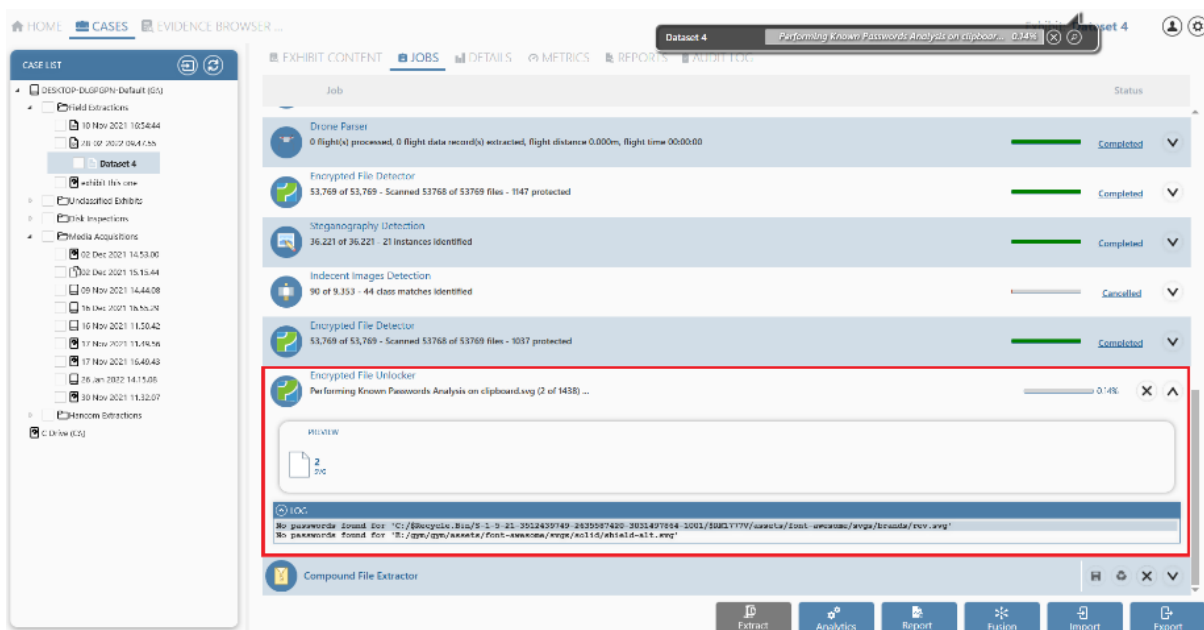
- Scroll down to the 'Password Processing' section from the Analytics window and select the 'Encrypted File Unlocker' job.

Figure 643



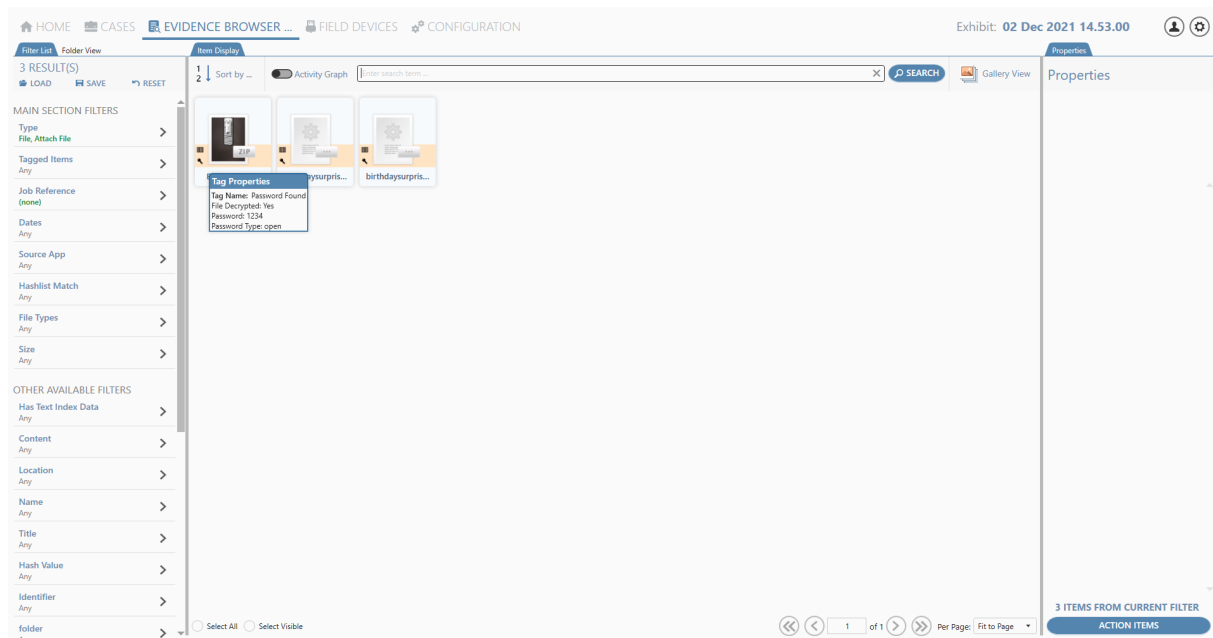
- Select START to run the job, and you will be taken to the JOBS tab to view the progress.

Figure 644



- Once the job has been completed, you can select VIEW RESULTS to go to the EVIDENCE BROWSER. Once the files are unlocked, you can unzip and extract them from the folders using the 'Compound File Extractor'.

Figure 645



6.16. REPORTS

Detego comes with several preconfigured reports, from a top-level look at a case's exhibits to the in-depth details of each exhibit in an investigation.

The 'Reports' tool rapidly filters through masses of data and parses the most useful intelligence so the operator can produce reports in HTML. Reports collect the exhibits from a case and display a file listing of the acquired data; they can also be configured to include audit logs and thumbnails of file artefacts (where possible). Some information that can be listed includes exhibit specifications, hash and keyword matches, websites visited, devices connected, identified usernames and passwords, downloaded files and password-protected containers and encryption.

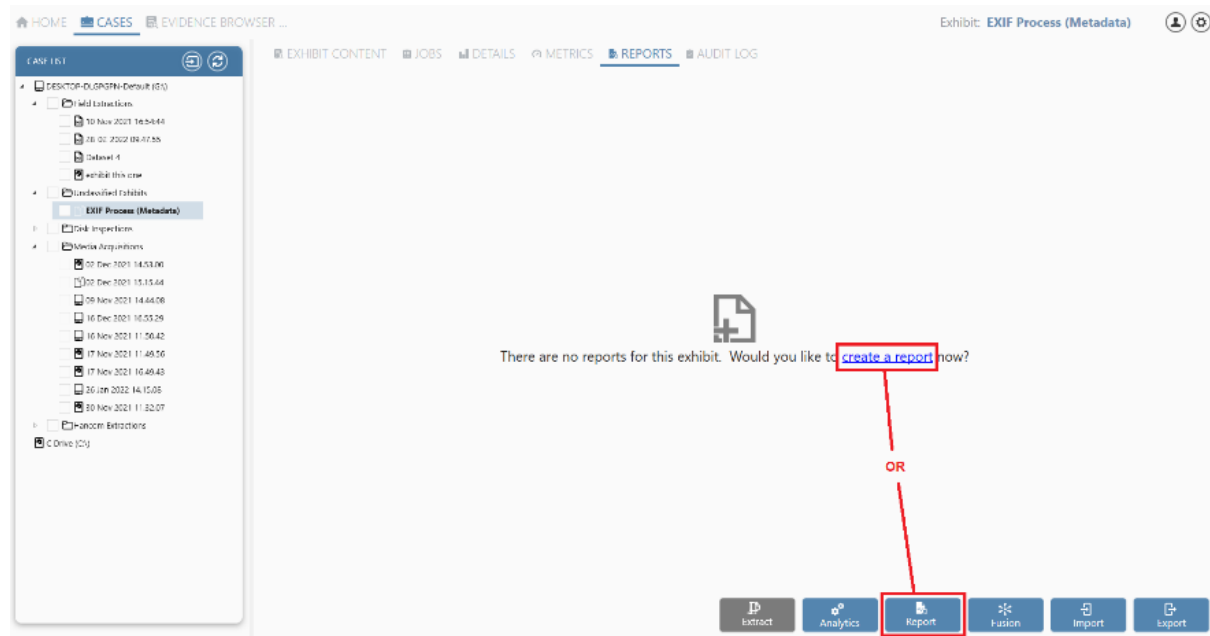
Also, the operator can now easily set up a click-of-a-button process that will acquire data from a device, analyse it and then generate reports from the intelligence gathered automatically, significantly speeding up the investigative process.

To access reports, follow these steps:

- Once an acquisition is complete, click the 'Analyse and Manage' tool tile from the Detego Analyse home screen.

- From the 'Cases' screen, click on the exhibit you wish to report and select either the 'Report' button from the bottom 'Actions' bar or open the 'Reports' tab and select the 'Create a report' text link.

Figure 646



- This will open a pop-up from which you can select the report type you want to generate.

DETEGO REPORT

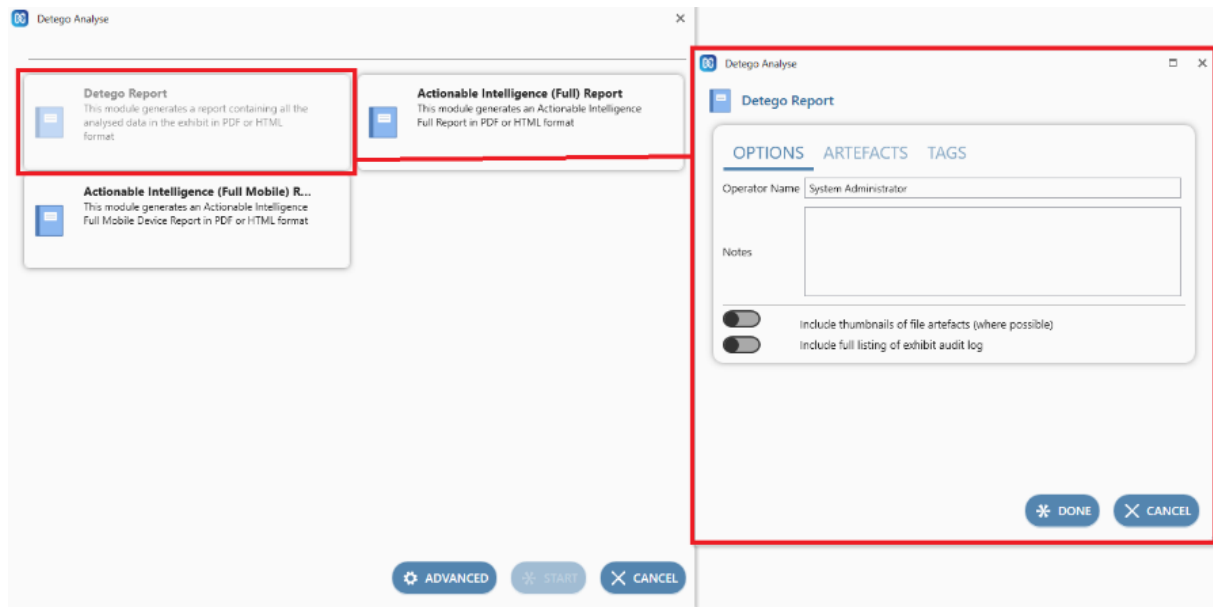
The 'Detego Report' contains detailed information about each exhibit in an investigation, including evidence summaries, listings and audit logs. It can be saved in HTML format (ready for exporting as PDF if required).

The report is generated from Detego, court-ready, with all the intelligence needed to prosecute a case.

To generate a 'Detego Report', follow these steps:

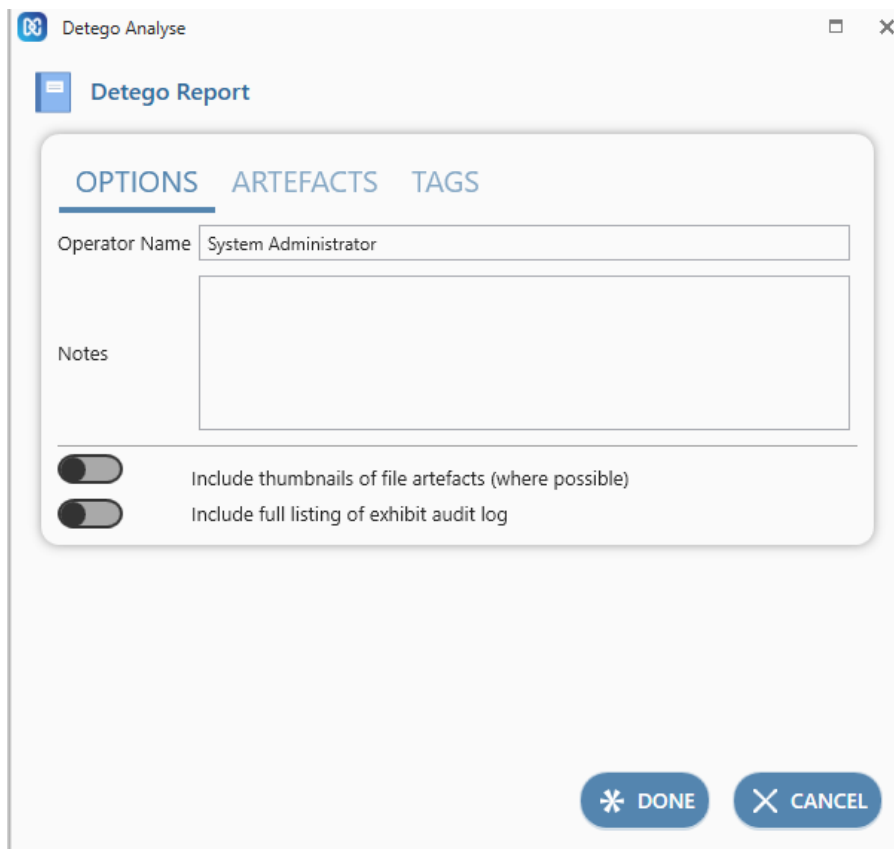
- Select the 'Detego Report' button from the report pop-up window to open the advanced options.

Figure 647



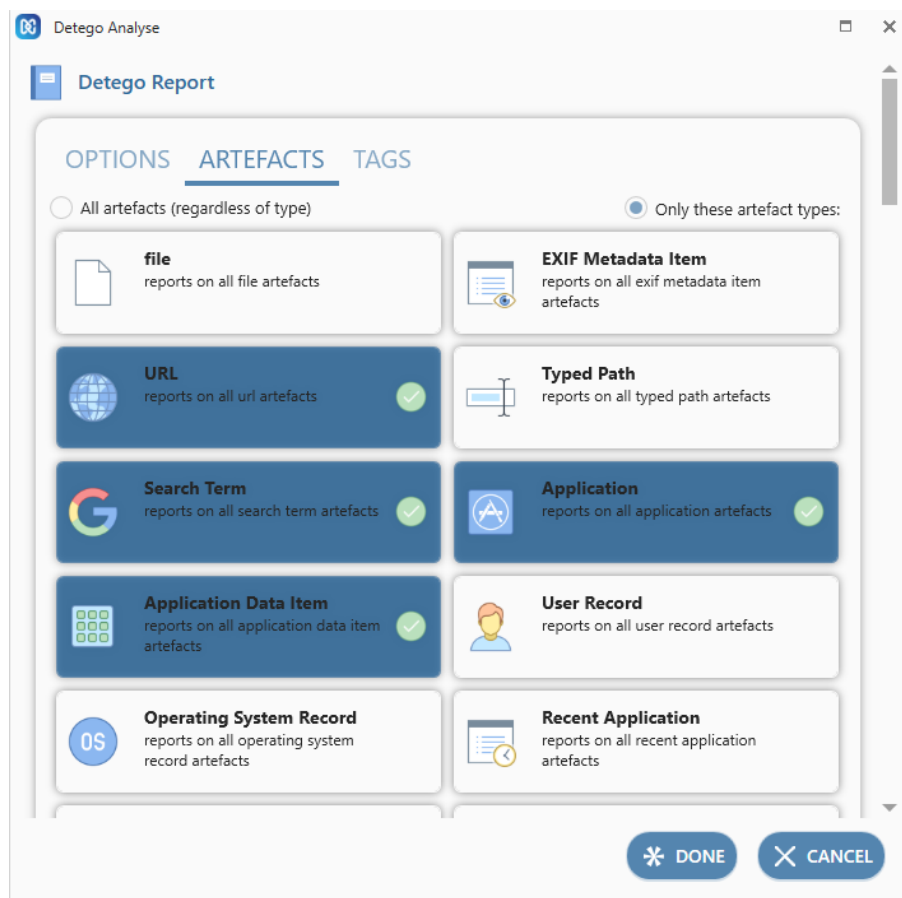
- In the 'Options' tab, enter an 'Operator Name' and any notes you want included in the report. Toggle on the two fields at the bottom of the window if you want to include thumbnails of file artefacts (where possible) and a full listing of the exhibit audit log.

Figure 648



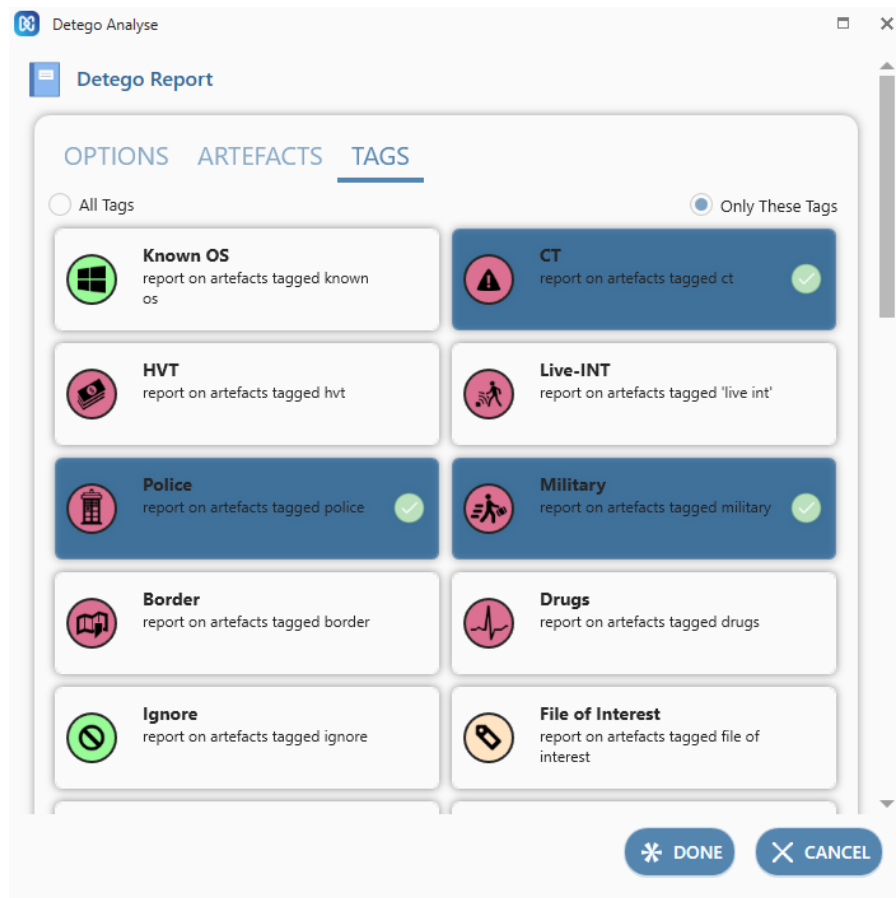
- The 'Artefacts' tab has two [2] radio buttons where the operator can choose whether the report lists all artefacts or specific types.
 - These types are File, EXIF Metadata Item, Uniform Resource Identifier, Typed Path, Search Term, Application, Application Data Item, User Record, Operating System Record, Recent Application, Recent File, Default Application, User Assist, USB Device Record, Hardware Entry, IP Address, Network Adapter, Network Connection, Connected Network, Executed Command, Physical Drive, Partition, Encryption Key, GPS Coordinate, Email, Bank Card, Contact, Contact Data Item, Call Event, Message, Fragment, Folder, Motherboard, Graphics Card, Processor, Memory Image, Credentials, Process, Local Directory, Remote Directory, Source Image, System Profile, Device Information Item, Account, Cookie, Download, Web Cache, Flight Path, Mobile Device, Task and Calendar.

Figure 649



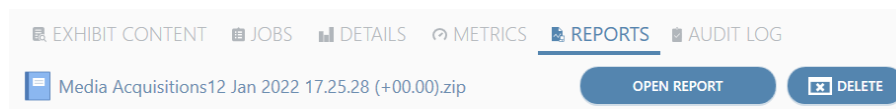
- The 'Tags' tab has two [2] radio buttons where the operator can choose whether the report lists all tags or only specific ones (both default and custom tags are available).

Figure 650



- Once you've completed your configurations, click the 'DONE' button in the bottom right corner of the pop-up. This will return you to the initial report pop-up, where a green tick icon will appear in the 'Detego Report' button. Click 'START'.
- Your report will then be generated and available to view and manage within Detego.

Figure 651



In addition to the existing Detego reports, we are introducing (as a preview version) a new style for reports, which will become the default in future releases:

Figure 652

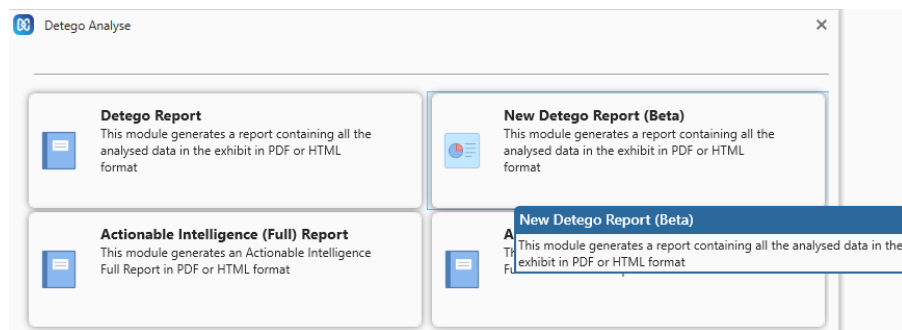
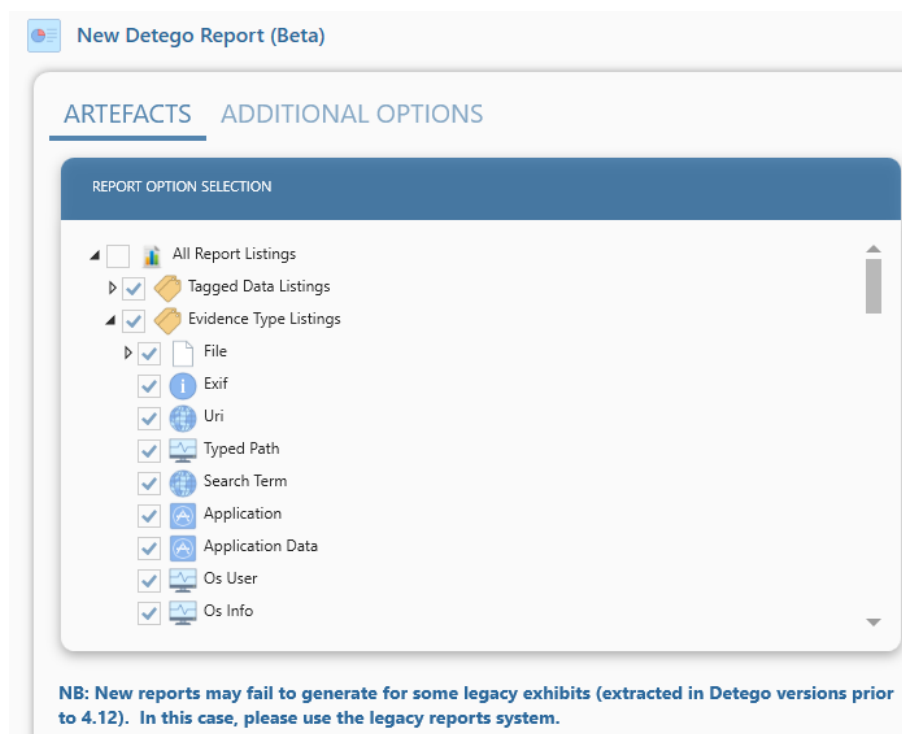
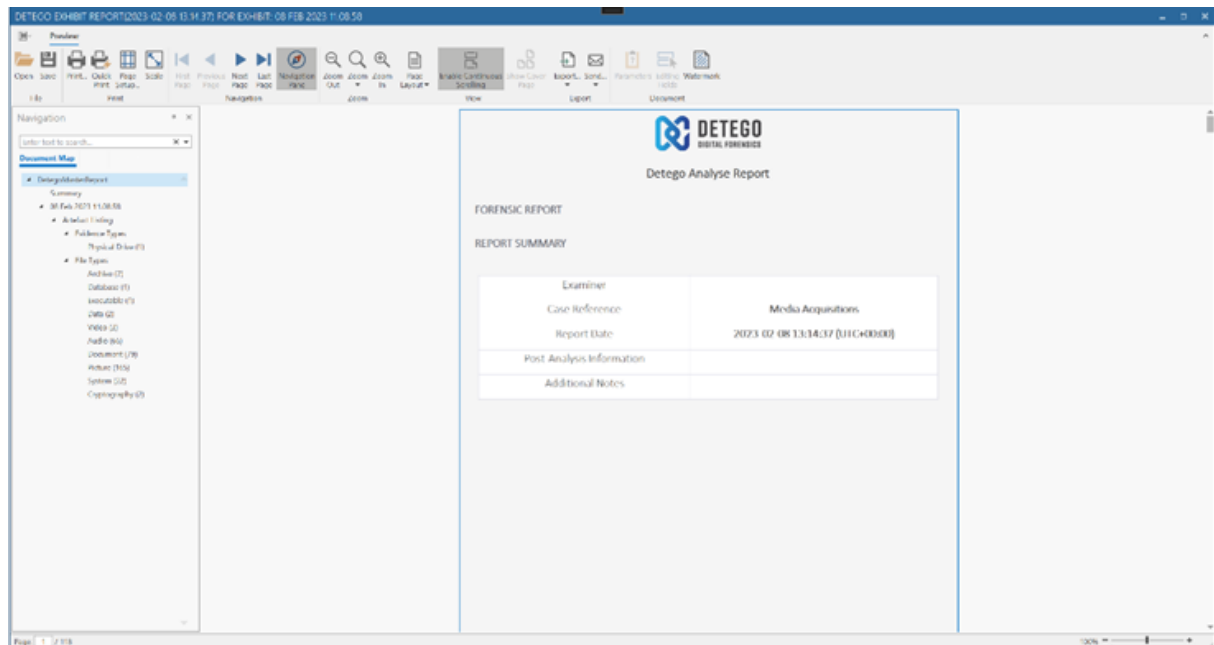


Figure 653



This report style has a new report viewer which allows the report to be browsed, saved, exported or printed:

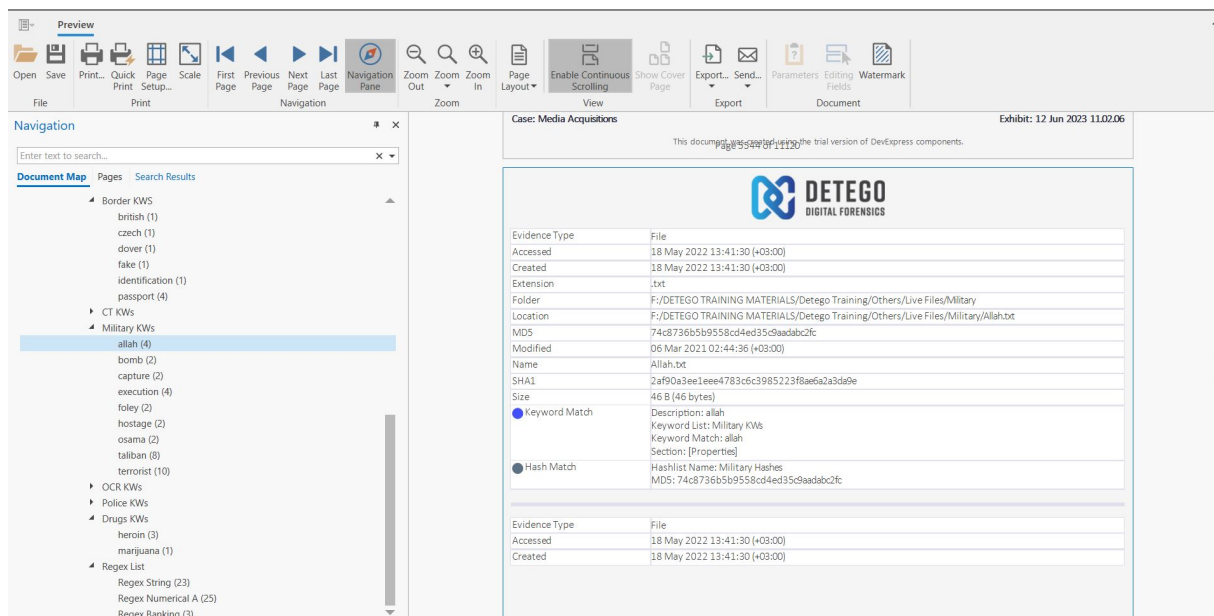
Figure 654



The following features were added to the **New Detego Report**

- Enable the user to show matching files for individual keywords & regex in separate sections in the report, as shown below. **This functionality is achieved by toggling on the “show matching files for individual keywords & regex in separate sections” button in the “Report Settings” tab, as shown below.**

Figure 655



- Enable the user to give a report a name with the option to add the current date as part of the report name, as shown below.

Figure 656

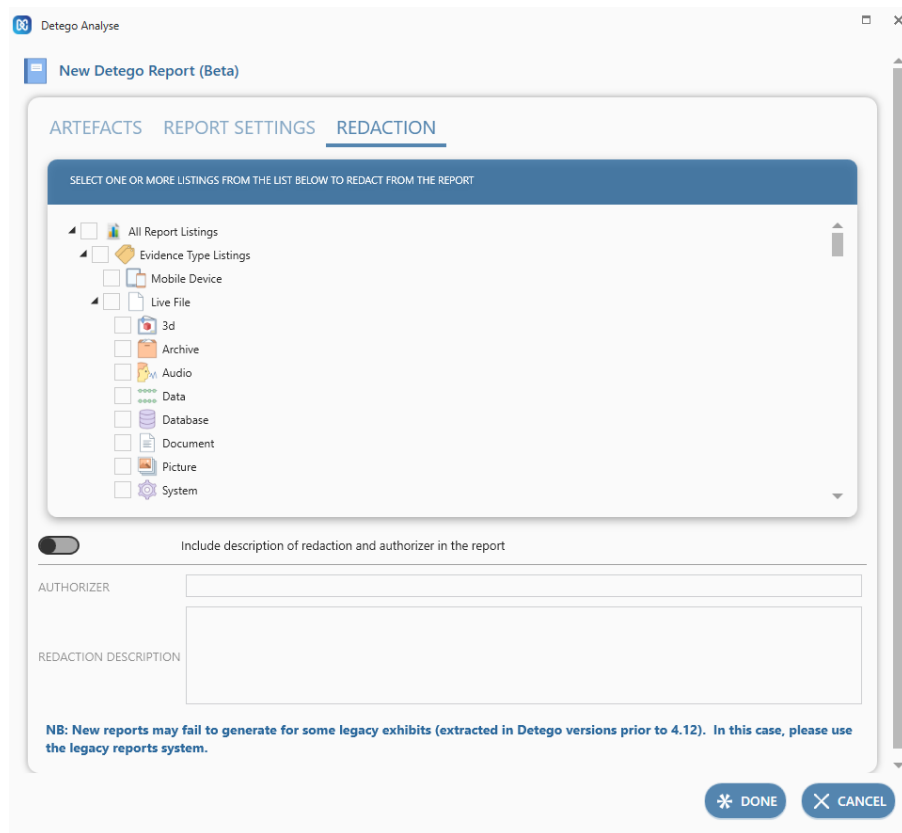
The screenshot shows the 'New Detego Report (Beta)' interface. At the top, there are three tabs: 'ARTEFACTS', 'REPORT SETTINGS' (which is selected and underlined), and 'REDACTION'. Below the tabs, there are several input fields and toggle switches:

- Report Name:** A text input field followed by a toggle switch labeled 'Include creation date/time in report name', which is currently turned on (green).
- Operator Name:** A text input field.
- NOTES:** A large text area for notes.
- Toggle switches for report content:**
 - 'Include thumbnails of file artefacts (where possible)': Turned off (grey).
 - 'Include full listing of exhibit audit log': Turned off (grey).
 - 'Show matching files for Individual Keywords & Regex in separate sections': Turned off (grey).
 - 'Include Supplementary Exhibit Metadata Files': Turned on (green).

At the bottom, there is a blue note: **NB: New reports may fail to generate for some legacy exhibits (extracted in Detego versions prior to 4.12). In this case, please use the legacy reports system.**

- Automatically expand all the report artefact listing groups on the report start page.
- Enable the user to report on hash matches and display them in a separate section in the report document map.
- Enable the user to show tagged data, evidence type, keyword match and regex listings in the respective exhibit.

Figure 657



- Select which items you wish to redact from the report.
- Once selected, you can type in your Authoriser name and any redaction notes.

SCREEN RECORDINGS INCLUDED

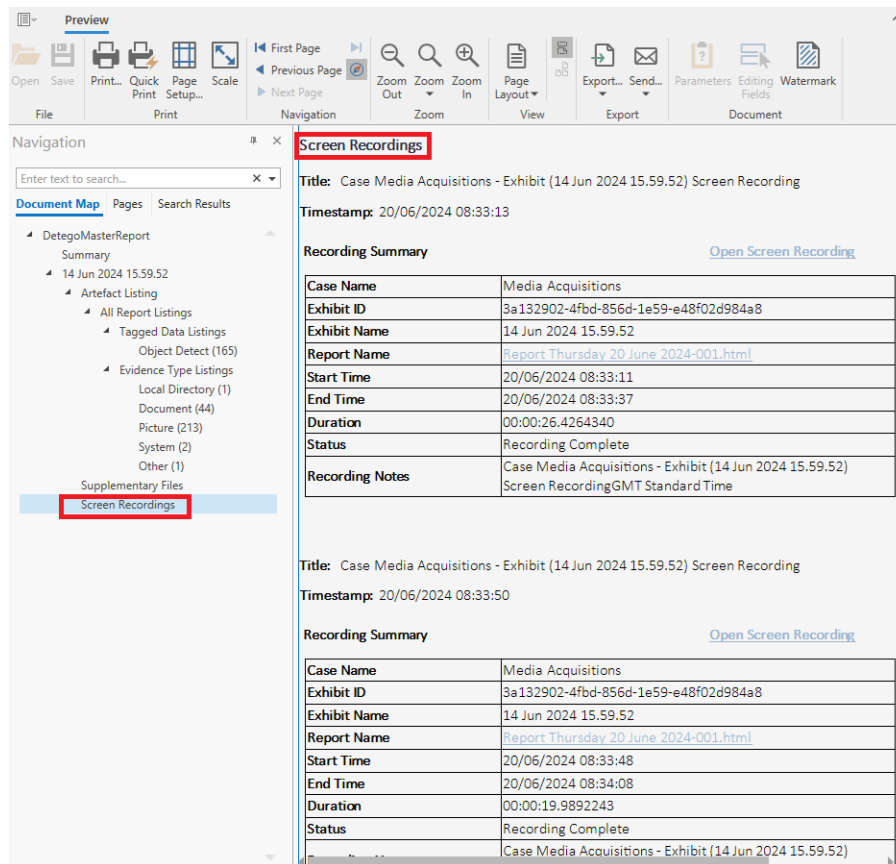
This feature enables inclusion of screen recording videos in Detego Analyse reports. When generating new reports, any screen recordings associated with the exhibit are included. The reports have a dedicated section for screen recordings in the document map, which provides detailed information and embedded links to the recordings and their summaries. These links remain active when the reports are exported to various formats like PDF, DOCX among others.

Include Screen Recordings

When generating new reports in Detego Analyse, any screen recordings that were recorded in the respective exhibit are automatically included in the report. This integration ensures that all relevant data, including screen recordings, is comprehensively documented. A new section for screen recordings is created in the document map as well as in the report itself. This section

provides a detailed overview of each screen recording included in the report. Refer to the figure below:

Figure 658



The screen recording section includes:

- **Recording Summary:** A brief overview of each screen recording.
- **Embedded Link to Video File:** A clickable link that opens the screen recording video file.
- **Embedded Link to Summary HTML File:** A clickable link that opens the summary HTML file associated with the recording.

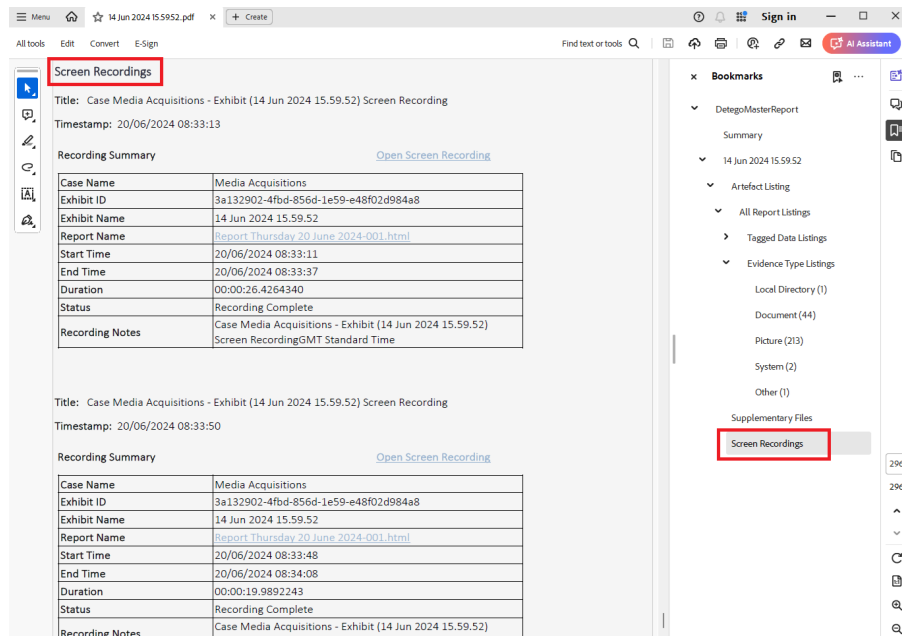
These details ensure that users can easily navigate to and view the screen recordings directly from the report.

Viewing Exported Reports

When the report is exported and opened in formats like PDF or DOCX, the links to the screen recordings and HTML summary file can be clicked to open the respective files.

It is important that the user's machine has the appropriate applications to open these files, such as HTML viewers or media players. Refer to the image below:

Figure 659



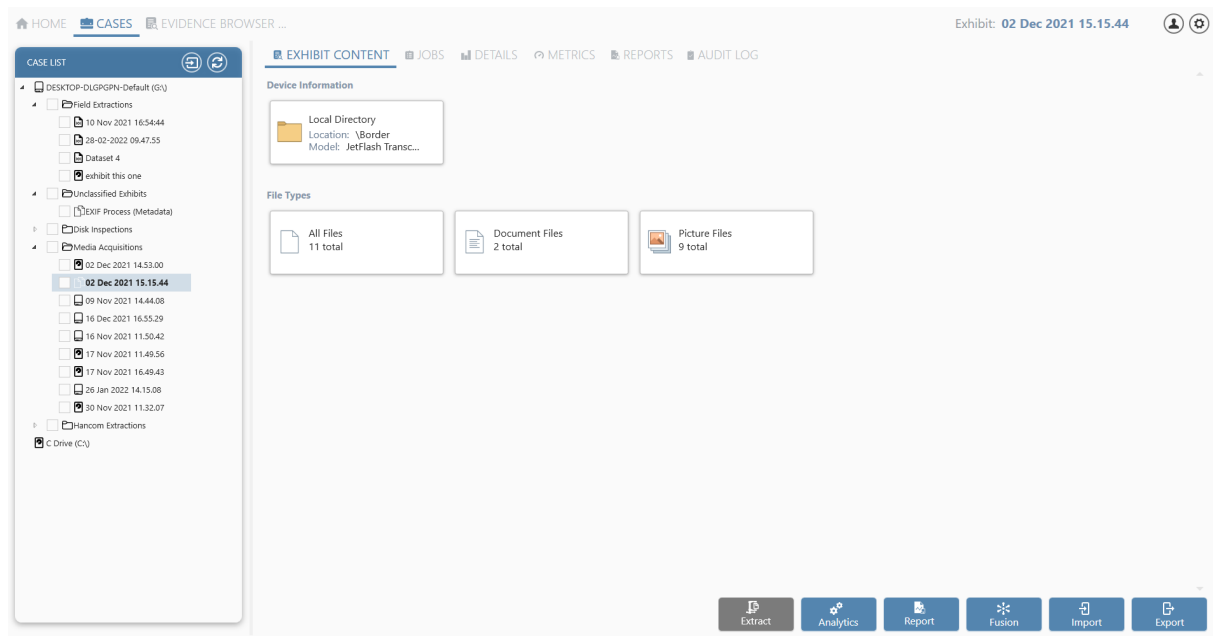
6.17. AUDIT LOG

Auditing allows the operator or third party to view audit logs across all cases, exhibits, and actions and create an audit report in an HTML format (ready to be printed to PDF if required). See the REPORTS section.

To access the 'Audit Log', follow these steps:

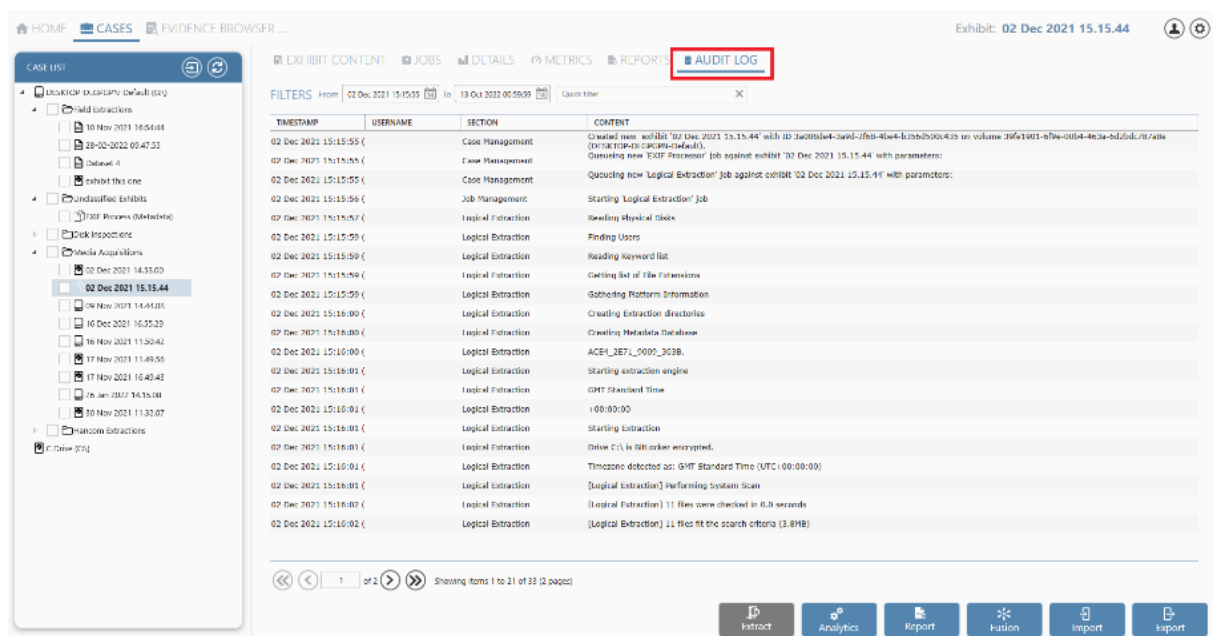
- From the Detego Analyse home screen, select the 'Analyse and Manage' tool tile.
- Select the exhibit you wish to view in the 'Cases' screen and click on the 'Audit Log' tab.

Figure 660



- The audit trail will then display the following information:
 - 'Timestamp' – The time and date when the action took place.
 - 'Section' – A description of the action.
 - 'Content' – Informative text about the actions that took place.

Figure 661



- At the top of the 'Audit Log' window, the operator can filter by date or enter a word or phrase into the search field.
- The bottom of the 'Audit Log' window shows the number of actions that have taken place and the number of pages to search through. Use the directional arrows to view different pages or navigate to a specific page, entering the page number into the page number textbox.

6.18. FUSION

Detego Fusion allows investigators to build a detailed intelligence picture of their exhibits, suspects and cases based on an advanced link analysis infrastructure. Detego Fusions' easily navigable interface allows a user to connect the dots to find 'needle-in-haystack' links across all of your digital exhibits, including computers, laptops (including Windows, Apple Mac & Linux systems), Mobile phones, Smartphones, Tablets, USB devices and other removable media (such as SD cards, portable external drives, IDE and SATA drives etc.) linked to a case, gaining valuable, previously un-associated evidence of links between people, places, devices and cases.

CENTRALISED CASE MANAGEMENT

The Detego Unified Forensics platform house all acquired case and exhibit data in a central location, the Detego Case Manager. Having all your cases and exhibits stored in a single location has many advantages; these include ease of backing up your data, ease in upgrading hardware when the time comes, ease of collaborative working (by taking advantage of the network-ready architecture that Detego is built on) and more importantly the ease with which the user can perform advanced link analysis on multiple cases to uncover hidden links between your cases and exhibits.

Detego Fusion will build these links by filtering through thousands of pre-configured variables in your data and displaying the links found in an intuitive interface that makes the work of the investigating officer easier.

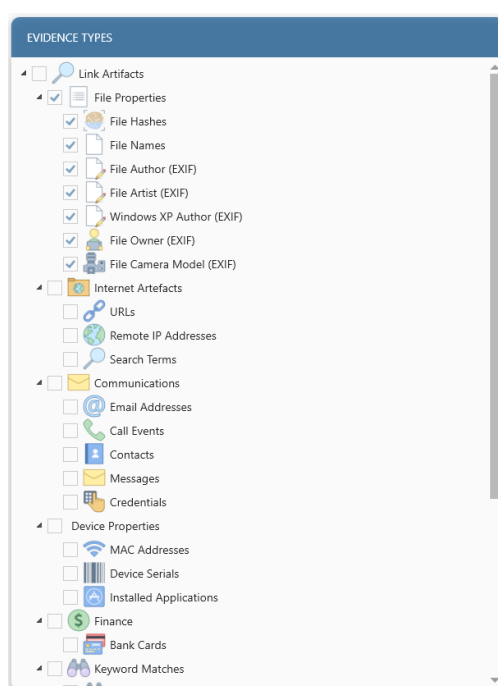
FUSION LINK ARTEFACTS

FILE PROPERTIES

FILE HASHES:

Fusion will filter through the hash values of the files in the exhibits you want to find links between. Detego stores file hash information by default. Therefore, link building based on file hashes can be done without running Detego Analytics processes.

Figure 662



FILE NAMES:

Fusion will filter through the file names in the exhibits you want links between. Link building based on file names can be done without running Detego Analytical processes.

EXIF METADATA:

EXIF Metadata in your data will give a wealth of information about a file. From running the EXIF processor analytics job, you will have access to image file capture data, camera details, geo data (if GPS was enabled on the capture device) and image editing software, among other pieces of

EXIF metadata stored on a file. Linking based on EXIF metadata is an easy way to show, for example, images that the same make and model of camera took.

MAPPING

GPS LOCATIONS:

GPS mapping data in images can be easily uncovered using the Detego Analytics EXIF Processor job. Access to all this information will enable building links based on images taken at locations close to each other while viewed on a map.

INTERNET ARTEFACTS

URLS:

The user will build links based on URLs visited on multiple target machines. In a few steps, you will be able to see suspects visiting the same obscure URLs, which may be the missing link in your case.

REMOTE IP ADDRESSES:

You can link cases and exhibits based on the remote IP addresses connected to a target machine.

SEARCH ITEMS:

The user can use the search terms stored on a target machine's browser history and utilise them as the filter to build links on similar search terms on multiple linked machines.

COMMUNICATIONS

EMAIL ADDRESSES:

Email communications made to and from the linked devices can be used as the filter with which links are built. Building the Analyse App Data analytics process will make this information available for linking purposes.

CALL EVENTS:

Running the Analyse App Data analytics process will make phone call data available for analysis. The user can then use call events as the filter with which links are built between two devices that are being investigated.

CONTACTS:

The contacts on investigated devices can be a way to link two crimes. By running the Analyse App Data analytics process, the information contained in a device's contacts database can be used as the filter to build links between multiple exhibits being investigated.

MESSAGES:

The Analyse App Data analytical process will make messages stored on a device available for search. Therefore, you can use these messages as the filter with which links are built between multiple devices under investigation.

CREDENTIALS:

The same credentials used to log in on multiple devices confirm that two devices are linked. You can quickly link two previously unconnected devices using credentials as the link filter. You can access the credentials data by running the Analyse App Data analytics process.

DEVICE PROPERTIES

MAC ADDRESSES:

A unique MAC address makes it easy to tell if the same device was recovered from multiple investigations. Being able to filter data and build links based on MAC addresses is a sure way to find devices used in previously unconnected exhibits.

DEVICE SERIALS:

Similar to MAC addresses, a device's unique serial number is an easy way of telling if the same device was recovered from multiple investigations. Filtering data and building links based on serial number matches is a way to find devices used in previously unconnected exhibits.

INSTALLED APPLICATIONS:

You can access data from the applications installed on your target devices by running the Analyse App Data analytical process. This makes it easy to use installed applications as the filter to build links in your cases.

FINANCE

BANK CARDS:

Detego can search through your exhibit data and pick out the bank card information contained in your data. This will allow you to use bank card data as a filter to build links between exhibits.

KEYWORD MATCHES

Saving all your exhibits that you have run keyword matches on stored in the Detego Case Manager will filter your data based on similar keyword match results.

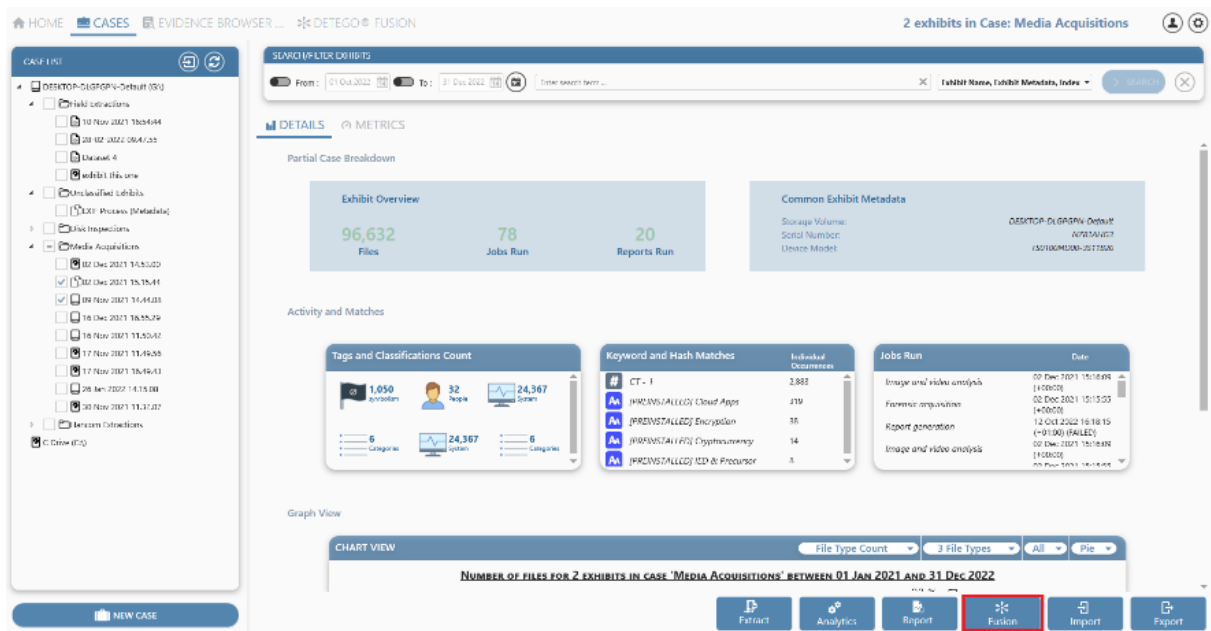
PERFORMING A FUSION LINK ANALYSIS

The process of performing link analysis between multiple exhibits is simple. In a few simple steps, you will have a graphical representation of the links between your exhibits and are digging deeper into these links.

The following steps will guide you as you perform your link analysis.

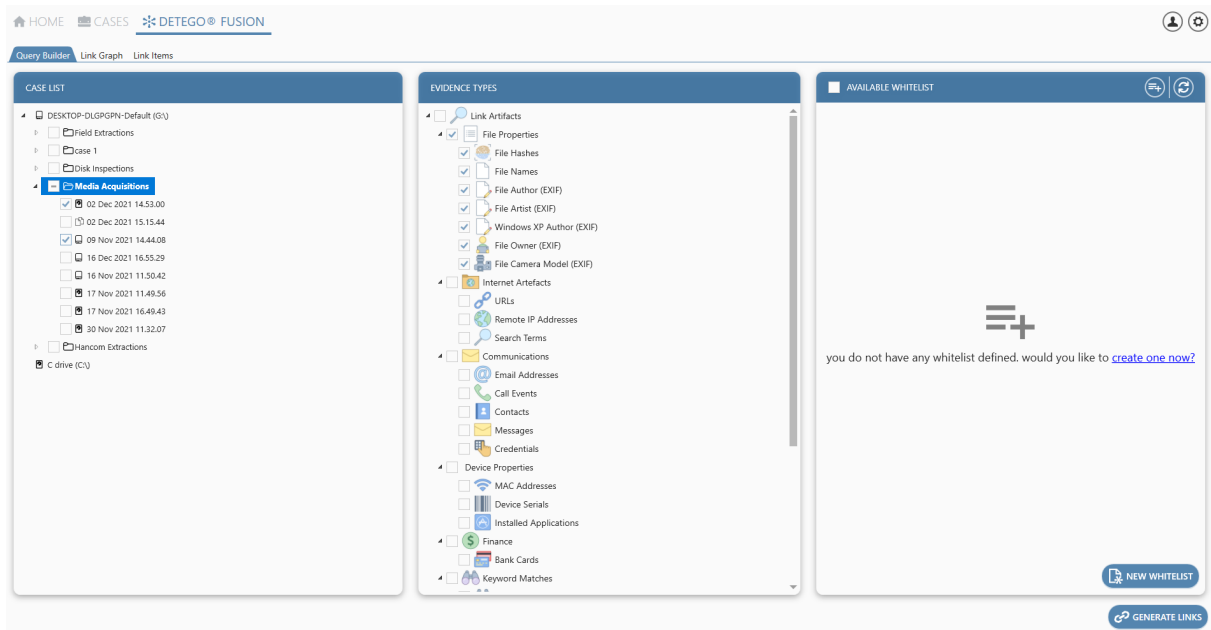
- From the Detego Analyse home screen, click on Analyse and Manage.
- The left-hand panel lists all of your current cases and exhibits. Navigate to the specific exhibits you want to build links on. Click on the checkbox to the left of your exhibits to select them.

Figure 663



- Click FUSION on the available tabs panel at the bottom of the case window. This will bring you to the Detego Fusion Query Builder.

Figure 664

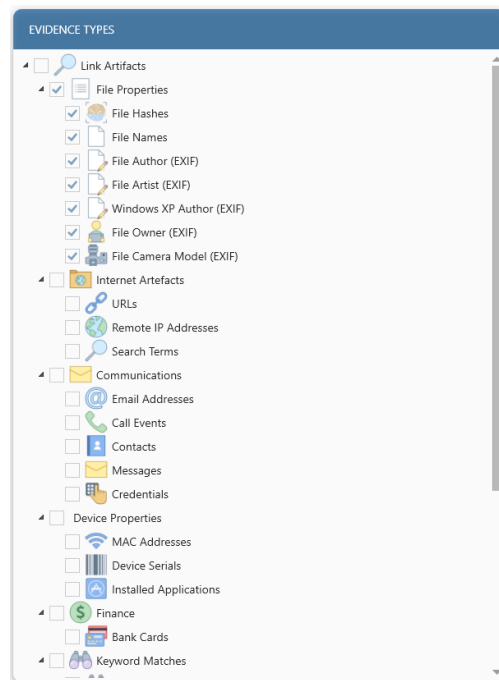


- The exhibits you selected will appear in the first column.
- Select what link artefacts you want to use to filter when building your links from the middle column.

- You can select as many artefacts as you wish.

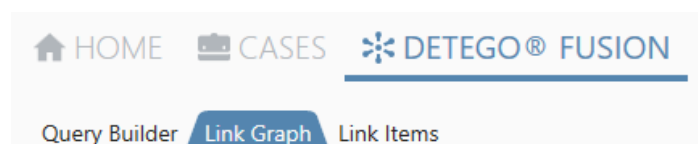
Note: The more exhibits & artefacts you select, the longer it will be for your link graph to be built.

Figure 665



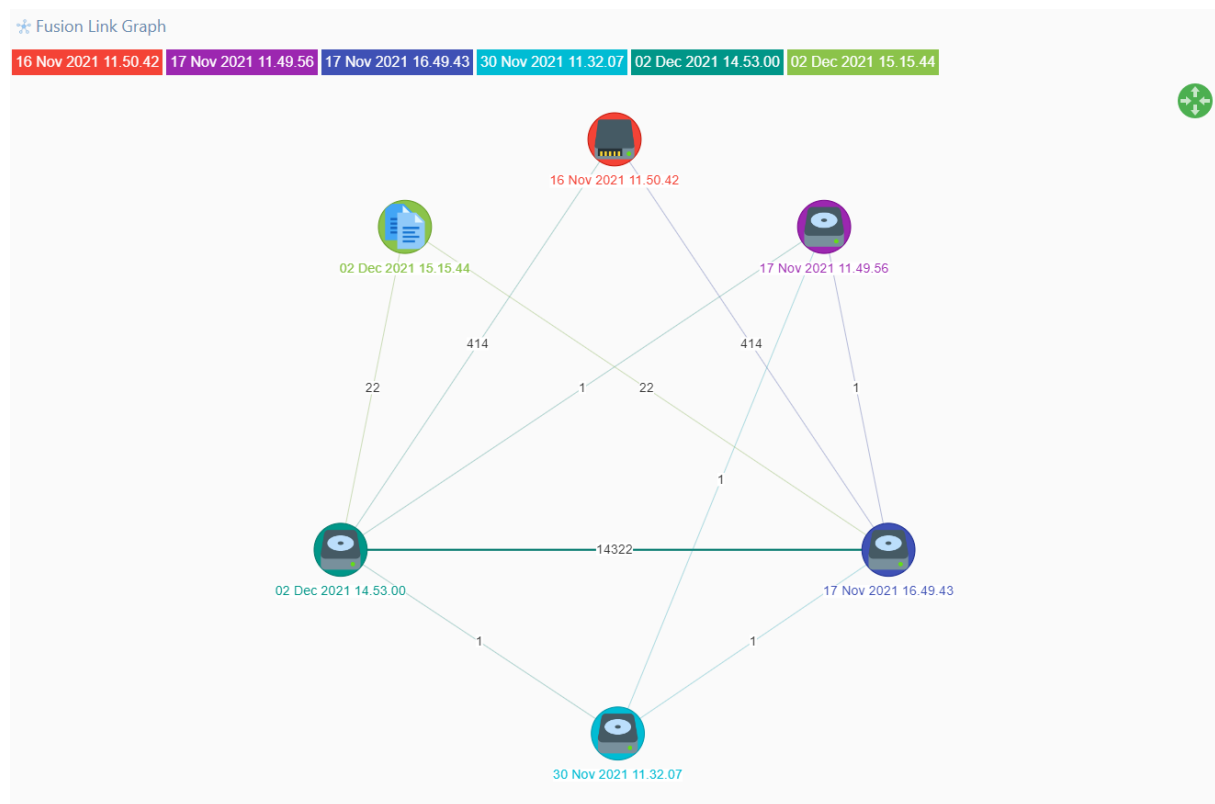
- From the right column, create a new whitelist or select from your available whitelists on terms you would like the link filter to ignore.
- When you have made your selections, click on GENERATE LINKS. A progress bar will appear at the top. Once link generation is complete, navigate to the LINK GRAPH TAB at the top left of the window.

Figure 666



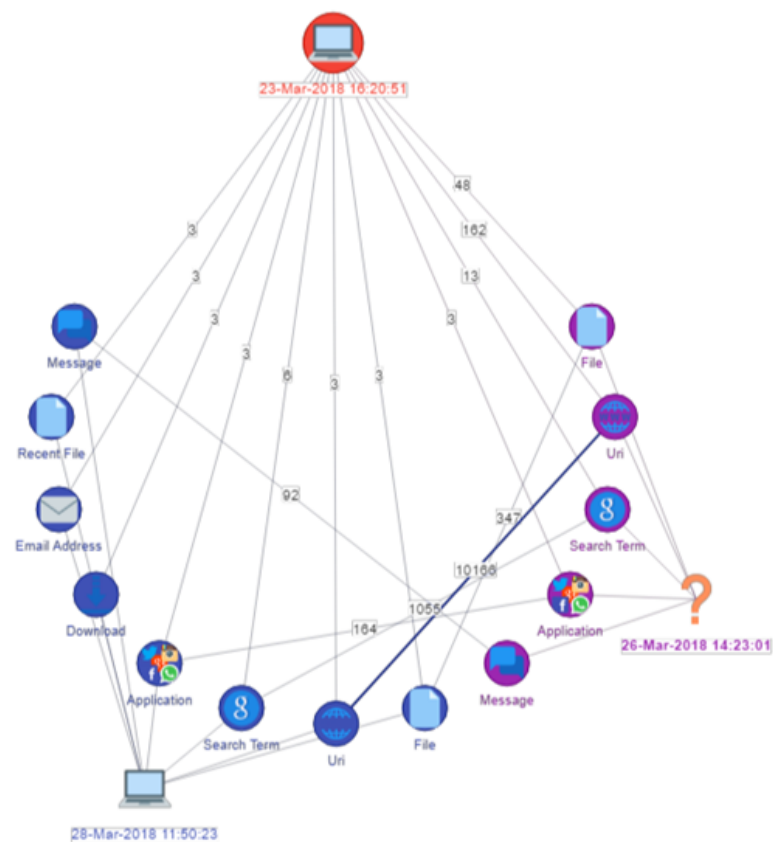
- On the left of the LINK GRAPH tab, you will find your existing Fusion Reports. They are listed with the most recently generated report appearing at the top. Select the report you would like to view.
- A link graph will appear on the right. At the top, you will find a colour-coded list of exhibits you are building links from. Below that, you will find the graphical link graph.

Figure 667



- There is a line extending from one exhibit to another. This indicates a link. Each line represents the number of links between the two exhibits.
- Double-clicking on any exhibits will expand the link graph to give a detailed view of the type of link artefacts discovered and the number of each evidence type discovered.

Figure 668



- Clicking link lines will display the Link Items between the two selected exhibits. The items are grouped for easy review below the link graph.

Figure 669

 Selected Links

File Hashes

 24 items available

File Names

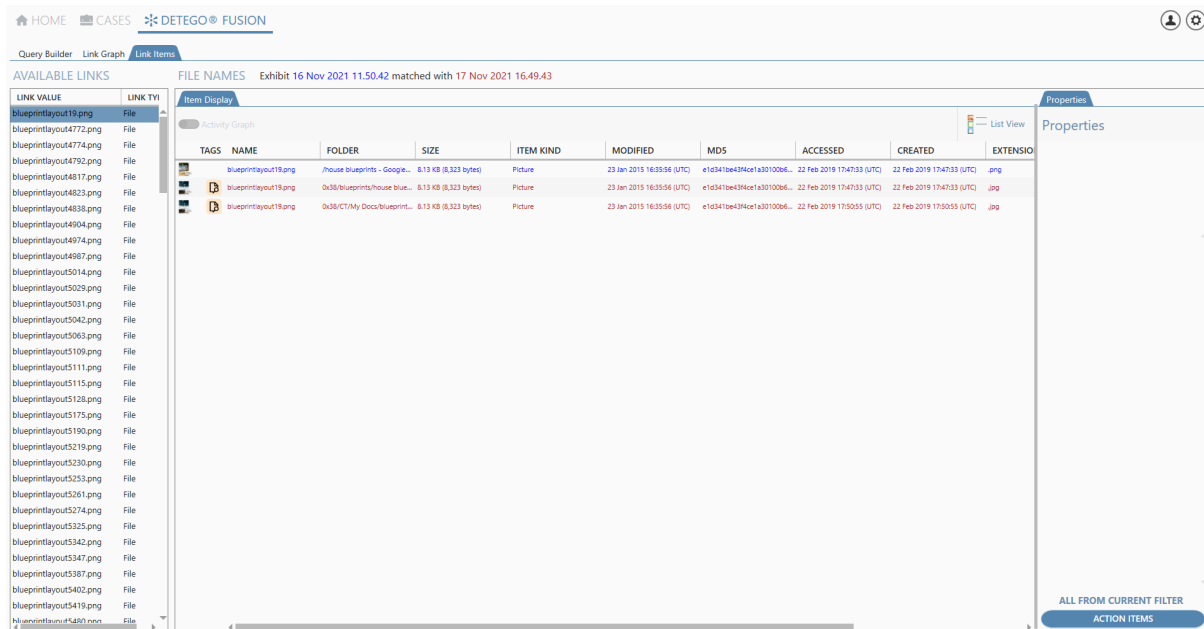
 19 items available

Credentials

 20 items available

- Clicking on link items, e.g., 'Installed Applications', will open the LINK ITEMS tab. Here, you see the 'Available links displayed on the right, the instances of the link item on each device in the middle and details about the link appearing on the right.

Figure 670



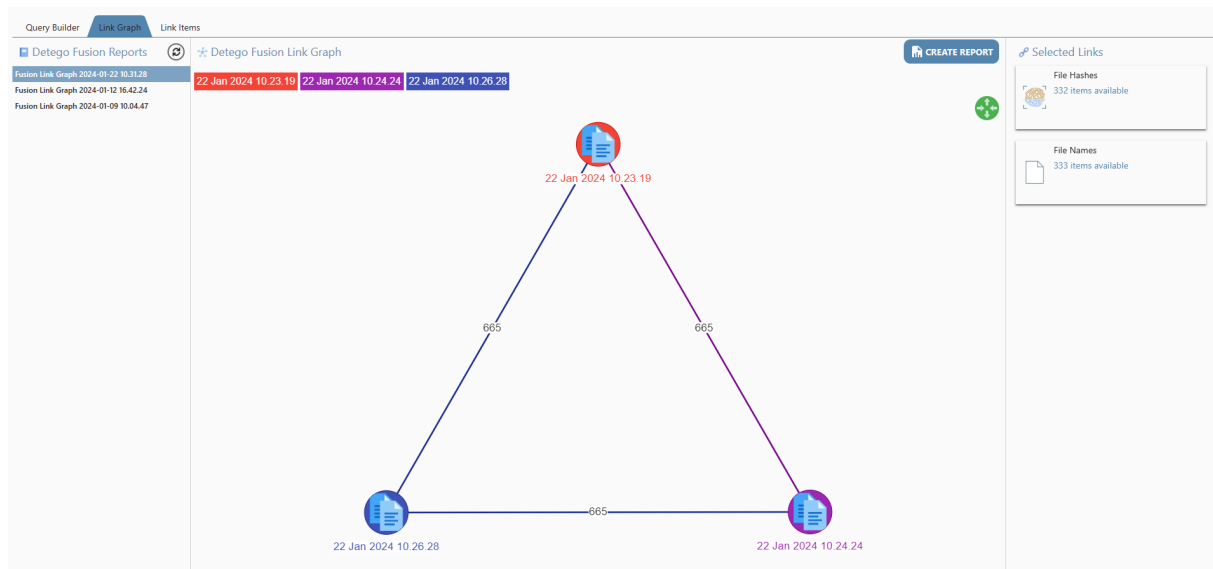
FUSION REPORT GENERATION IN EXCEL AND CSV FORMATS

This feature introduces enhanced functionality for report generation within Detego Analyse AI+. Users can seamlessly create **Fusion reports** in **Excel** and **CSV** formats. This process empowers users to generate comprehensive reports encompassing either all Fusion links or a specific Fusion link of their choice.

USER INTERFACE:

In the displayed Fusion Link Graph, users have the option to create reports by utilising the **"Create Report"** button. This button triggers a pop-up window, offering users a range of customisation options for report generation.

Figure 671



REPORT GENERATION OPTIONS POP-UP WINDOW

In the pop-up window, users are presented with the following options:

- **Toggle EXCEL Button:**

Use the toggle button to indicate whether an Excel report should be generated.

- **Toggle CSV Button:**

Employ the toggle button to specify whether a CSV report should be generated.

- **Destination Directory Selection:** Choose the directory where the resulting report files will be stored.

By incorporating these options, users have precise control over the report generation process, tailoring it to their specific needs and preferences.

Figure 672

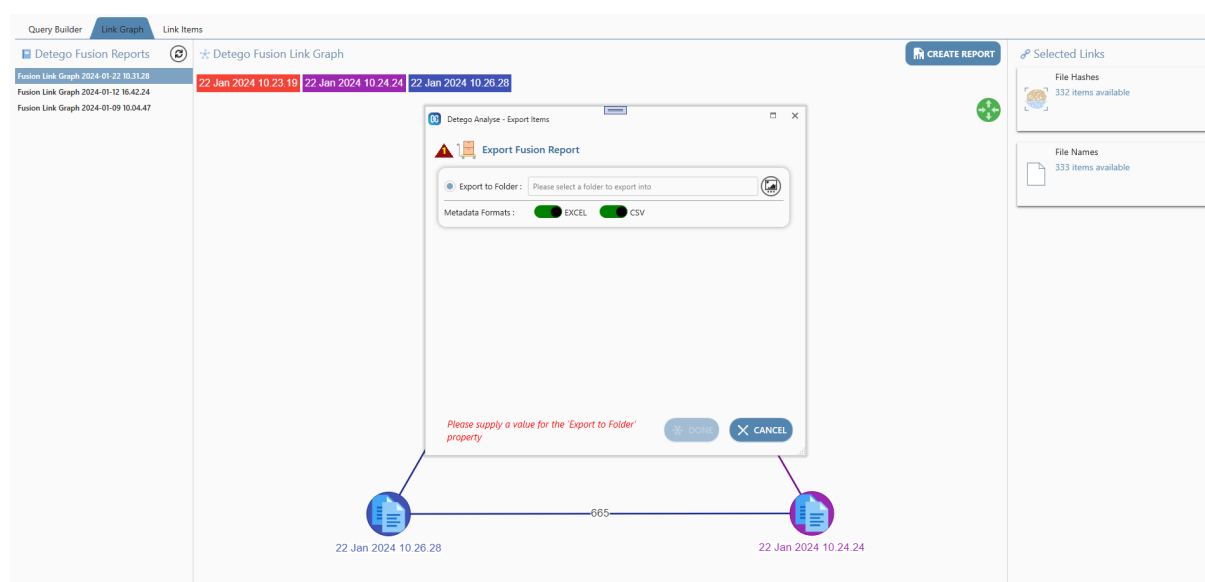


Figure 673

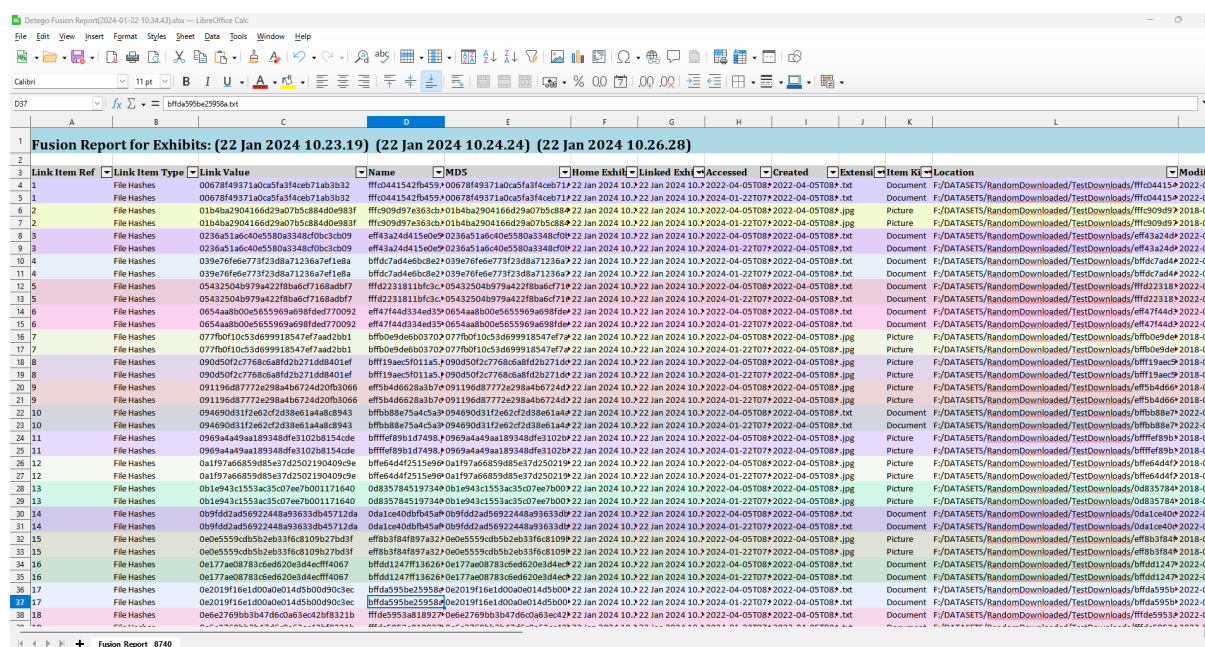


Figure 674

Link Item	Link Type	Link Value	Name	MD5	Home Exhibit	Linked Exhibit	Accessed	Created	Extension	Item Kind	Location
1	File Hashes	0067849371a0ca5a34ceb71ab3b32	0067849371a0ca5a34ceb71ab3b32	0067849371a0ca5a34ceb71ab3b32	22 Jan 2024 10:23:19	22 Jan 2024 10:23:19	2022-04-05T08:25:04	2022-04-05T08:25:04	txt	Document	F:/DATASETS/RandomDownloaded/TestDownloads/ffc0441542b2459.txt
2	File Hashes	0067849371a0ca5a34ceb71ab3b32	0067849371a0ca5a34ceb71ab3b32	0067849371a0ca5a34ceb71ab3b32	22 Jan 2024 10:23:19	22 Jan 2024 10:23:19	2022-04-05T08:25:04	2022-04-05T08:25:04	txt	Document	F:/DATASETS/RandomDownloaded/TestDownloads/ffc0441542b2459.txt
3	File Hashes	01b4ba2904166d09a07b5c884d0e983f	01b4ba2904166d09a07b5c884d0e983f	01b4ba2904166d09a07b5c884d0e983f	22 Jan 2024 10:23:19	22 Jan 2024 10:23:19	2022-04-05T08:25:04	2022-04-05T08:25:04	jpg	Picture	F:/DATASETS/RandomDownloaded/TestDownloads/ffc009d97e363cb.jpg
4	File Hashes	01b4ba2904166d09a07b5c884d0e983f	01b4ba2904166d09a07b5c884d0e983f	01b4ba2904166d09a07b5c884d0e983f	22 Jan 2024 10:23:19	22 Jan 2024 10:23:19	2022-04-05T08:25:04	2022-04-05T08:25:04	jpg	Picture	F:/DATASETS/RandomDownloaded/TestDownloads/ffc009d97e363cb.jpg
5	File Hashes	0236a51a6c40e5580a3348c0bc3c009	0236a51a6c40e5580a3348c0bc3c009	0236a51a6c40e5580a3348c0bc3c009	22 Jan 2024 10:23:19	22 Jan 2024 10:23:19	2022-04-05T08:25:02	2022-04-05T08:25:02	txt	Document	F:/DATASETS/RandomDownloaded/TestDownloads/efh43a244415e0w5.txt
6	File Hashes	0236a51a6c40e5580a3348c0bc3c009	0236a51a6c40e5580a3348c0bc3c009	0236a51a6c40e5580a3348c0bc3c009	22 Jan 2024 10:23:19	22 Jan 2024 10:23:19	2022-04-05T08:25:02	2022-04-05T08:25:02	txt	Document	F:/DATASETS/RandomDownloaded/TestDownloads/efh43a244415e0w5.txt
7	File Hashes	0236a51a6c40e5580a3348c0bc3c009	0236a51a6c40e5580a3348c0bc3c009	0236a51a6c40e5580a3348c0bc3c009	22 Jan 2024 10:23:19	22 Jan 2024 10:23:19	2022-04-05T08:25:02	2022-04-05T08:25:02	txt	Document	F:/DATASETS/RandomDownloaded/TestDownloads/efh43a244415e0w5.txt
8	File Hashes	039e78fe6773f2328a71239a7ef1e8a	039e78fe6773f2328a71239a7ef1e8a	039e78fe6773f2328a71239a7ef1e8a	22 Jan 2024 10:23:19	22 Jan 2024 10:23:19	2022-04-05T08:24:52	2022-04-05T08:24:52	txt	Document	F:/DATASETS/RandomDownloaded/TestDownloads/bfbc7a4d46bcb2.txt
9	File Hashes	039e78fe6773f2328a71239a7ef1e8a	039e78fe6773f2328a71239a7ef1e8a	039e78fe6773f2328a71239a7ef1e8a	22 Jan 2024 10:23:19	22 Jan 2024 10:23:19	2022-04-05T08:24:52	2022-04-05T08:24:52	txt	Document	F:/DATASETS/RandomDownloaded/TestDownloads/bfbc7a4d46bcb2.txt
10	File Hashes	06432504b979a42208a6c71168adbf7	06432504b979a42208a6c71168adbf7	06432504b979a42208a6c71168adbf7	22 Jan 2024 10:23:19	22 Jan 2024 10:23:19	2022-04-05T08:25:06	2022-04-05T08:25:06	txt	Document	F:/DATASETS/RandomDownloaded/TestDownloads/ffc2213111f6c3.txt
11	File Hashes	06432504b979a42208a6c71168adbf7	06432504b979a42208a6c71168adbf7	06432504b979a42208a6c71168adbf7	22 Jan 2024 10:23:19	22 Jan 2024 10:23:19	2022-04-05T08:25:06	2022-04-05T08:25:06	txt	Document	F:/DATASETS/RandomDownloaded/TestDownloads/ffc2213111f6c3.txt
12	File Hashes	06432504b979a42208a6c71168adbf7	06432504b979a42208a6c71168adbf7	06432504b979a42208a6c71168adbf7	22 Jan 2024 10:23:19	22 Jan 2024 10:23:19	2022-04-05T08:25:06	2022-04-05T08:25:06	txt	Document	F:/DATASETS/RandomDownloaded/TestDownloads/ffc2213111f6c3.txt
13	File Hashes	0654aa80e565569a6989ded770092	0654aa80e565569a6989ded770092	0654aa80e565569a6989ded770092	22 Jan 2024 10:23:19	22 Jan 2024 10:23:19	2022-04-05T08:25:02	2022-04-05T08:25:02	txt	Document	F:/DATASETS/RandomDownloaded/TestDownloads/efh4744d334ed35.txt
14	File Hashes	0654aa80e565569a6989ded770092	0654aa80e565569a6989ded770092	0654aa80e565569a6989ded770092	22 Jan 2024 10:23:19	22 Jan 2024 10:23:19	2022-04-05T08:25:02	2022-04-05T08:25:02	txt	Document	F:/DATASETS/RandomDownloaded/TestDownloads/efh4744d334ed35.txt
15	File Hashes	077bf0f10c53d699918547ef7aad2b01	077bf0f10c53d699918547ef7aad2b01	077bf0f10c53d699918547ef7aad2b01	22 Jan 2024 10:23:19	22 Jan 2024 10:23:19	2022-04-05T08:24:52	2022-04-05T08:24:52	jpg	Picture	F:/DATASETS/RandomDownloaded/TestDownloads/bfbc0e6de6a03702.jpg
16	File Hashes	077bf0f10c53d699918547ef7aad2b01	077bf0f10c53d699918547ef7aad2b01	077bf0f10c53d699918547ef7aad2b01	22 Jan 2024 10:23:19	22 Jan 2024 10:23:19	2022-04-05T08:24:52	2022-04-05T08:24:52	jpg	Picture	F:/DATASETS/RandomDownloaded/TestDownloads/bfbc0e6de6a03702.jpg
17	File Hashes	090f5092c7768c6a8d2b271d68401ef	090f5092c7768c6a8d2b271d68401ef	090f5092c7768c6a8d2b271d68401ef	22 Jan 2024 10:23:19	22 Jan 2024 10:23:19	2022-04-05T08:24:58	2022-04-05T08:24:58	jpg	Picture	F:/DATASETS/RandomDownloaded/TestDownloads/bfbc19a5c5011a5.jpg
18	File Hashes	090f5092c7768c6a8d2b271d68401ef	090f5092c7768c6a8d2b271d68401ef	090f5092c7768c6a8d2b271d68401ef	22 Jan 2024 10:23:19	22 Jan 2024 10:23:19	2022-04-05T08:24:58	2022-04-05T08:24:58	jpg	Picture	F:/DATASETS/RandomDownloaded/TestDownloads/bfbc19a5c5011a5.jpg
19	File Hashes	091196d87772e298a4b6724d20b3066	091196d87772e298a4b6724d20b3066	091196d87772e298a4b6724d20b3066	22 Jan 2024 10:23:19	22 Jan 2024 10:23:19	2022-04-05T08:25:03	2022-04-05T08:25:03	jpg	Picture	F:/DATASETS/RandomDownloaded/TestDownloads/efh5b4d6628a3b7c.jpg
20	File Hashes	091196d87772e298a4b6724d20b3066	091196d87772e298a4b6724d20b3066	091196d87772e298a4b6724d20b3066	22 Jan 2024 10:23:19	22 Jan 2024 10:23:19	2022-04-05T08:25:03	2022-04-05T08:25:03	jpg	Picture	F:/DATASETS/RandomDownloaded/TestDownloads/efh5b4d6628a3b7c.jpg
21	File Hashes	091196d87772e298a4b6724d20b3066	091196d87772e298a4b6724d20b3066	091196d87772e298a4b6724d20b3066	22 Jan 2024 10:23:19	22 Jan 2024 10:23:19	2022-04-05T08:25:03	2022-04-05T08:25:03	jpg	Picture	F:/DATASETS/RandomDownloaded/TestDownloads/efh5b4d6628a3b7c.jpg
22	File Hashes	0969a4a9aa189348df63102b6154cde	0969a4a9aa189348df63102b6154cde	0969a4a9aa189348df63102b6154cde	22 Jan 2024 10:23:19	22 Jan 2024 10:23:19	2022-04-05T08:25:00	2022-04-05T08:25:00	jpg	Picture	F:/DATASETS/RandomDownloaded/TestDownloads/bfbcf6f89b1d7408.jpg
23	File Hashes	0969a4a9aa189348df63102b6154cde	0969a4a9aa189348df63102b6154cde	0969a4a9aa189348df63102b6154cde	22 Jan 2024 10:23:19	22 Jan 2024 10:23:19	2022-04-05T08:25:00	2022-04-05T08:25:00	jpg	Picture	F:/DATASETS/RandomDownloaded/TestDownloads/bfbcf6f89b1d7408.jpg
24	File Hashes	0969a4a9aa189348df63102b6154cde	0969a4a9aa189348df63102b6154cde	0969a4a9aa189348df63102b6154cde	22 Jan 2024 10:23:19	22 Jan 2024 10:23:19	2022-04-05T08:25:00	2022-04-05T08:25:00	jpg	Picture	F:/DATASETS/RandomDownloaded/TestDownloads/bfbcf6f89b1d7408.jpg
25	File Hashes	0a197a68589a5e37d2502190409cde	0a197a68589a5e37d2502190409cde	0a197a68589a5e37d2502190409cde	22 Jan 2024 10:23:19	22 Jan 2024 10:23:19	2022-04-05T08:24:55	2022-04-05T08:24:55	jpg	Picture	F:/DATASETS/RandomDownloaded/TestDownloads/bfbc644d2515e96.jpg
26	File Hashes	0a197a68589a5e37d2502190409cde	0a197a68589a5e37d2502190409cde	0a197a68589a5e37d2502190409cde	22 Jan 2024 10:23:19	22 Jan 2024 10:23:19	2022-04-05T08:24:55	2022-04-05T08:24:55	jpg	Picture	F:/DATASETS/RandomDownloaded/TestDownloads/bfbc644d2515e96.jpg
27	File Hashes	0a197a68589a5e37d2502190409cde	0a197a68589a5e37d2502190409cde	0a197a68589a5e37d2502190409cde	22 Jan 2024 10:23:19	22 Jan 2024 10:23:19	2022-04-05T08:24:55	2022-04-05T08:24:55	jpg	Picture	F:/DATASETS/RandomDownloaded/TestDownloads/bfbc644d2515e96.jpg
28	File Hashes	0b1e943c1553ac35c07ee7b00117164	0b1e943c1553ac35c07ee7b00117164	0b1e943c1553ac35c07ee7b00117164	22 Jan 2024 10:23:19	22 Jan 2024 10:23:19	2022-04-05T08:24:50	2022-04-05T08:24:50	jpg	Picture	F:/DATASETS/RandomDownloaded/TestDownloads/0a63578451973405.jpg
29	File Hashes	0b1e943c1553ac35c07ee7b00117164	0b1e943c1553ac35c07ee7b00117164	0b1e943c1553ac35c07ee7b00117164	22 Jan 2024 10:23:19	22 Jan 2024 10:23:19	2022-04-05T08:24:50	2022-04-05T08:24:50	txt	Document	F:/DATASETS/RandomDownloaded/TestDownloads/0a63578451973405.txt

The two figures above showcase exemplary reports generated using this feature. Users can create detailed Excel and CSV reports, capturing all relevant links based on their selection in the Fusion-Link Graph.

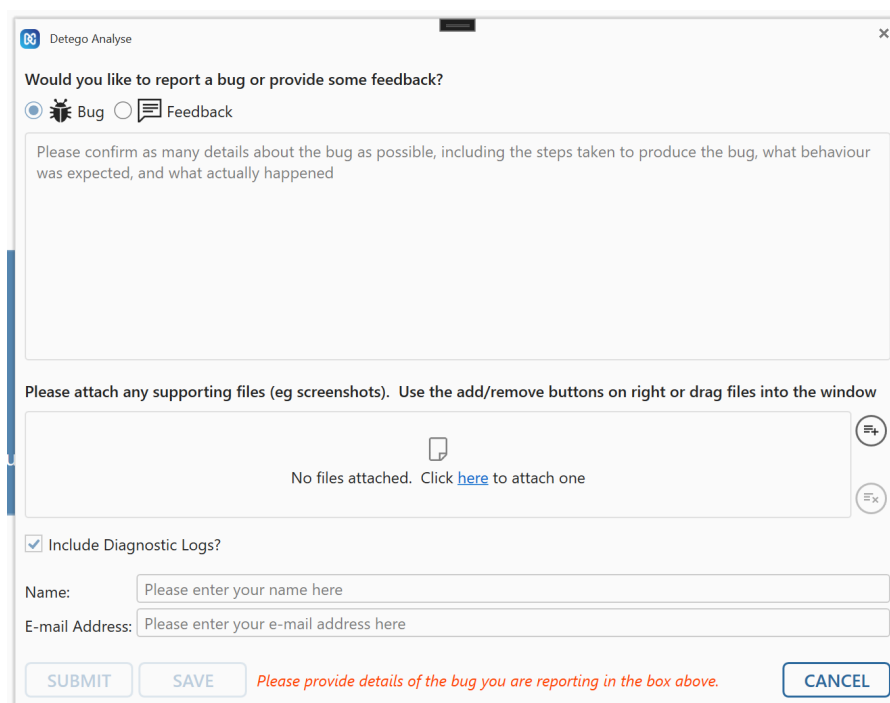
The same process can be followed to generate Fusion reports for a specific link within the Fusion-Link Items Tab.

This feature enhances user flexibility and efficiency in managing and extracting valuable insights from Fusion links, contributing to a more streamlined and effective reporting process.

7. TROUBLESHOOTING

A new mechanism for reporting issues and user feedback has been implemented in this build. The following new dialog will be used whenever an exception occurs during the operation of Detego or if the user clicks on the new feedback button in the title bar:

Figure 675



The screenshot shows a Windows-style dialog box titled "Detego Analyse". It contains the following elements:

- A title bar with the text "Detego Analyse" and a close button (X).
- A question: "Would you like to report a bug or provide some feedback?".
- Two radio buttons: "Bug" (selected) and "Feedback".
- A large text area with the instruction: "Please confirm as many details about the bug as possible, including the steps taken to produce the bug, what behaviour was expected, and what actually happened".
- A section for attaching files with the instruction: "Please attach any supporting files (eg screenshots). Use the add/remove buttons on right or drag files into the window". It shows a file icon and the text "No files attached. Click [here](#) to attach one".
- A checkbox labeled "Include Diagnostic Logs?" which is checked.
- Input fields for "Name:" and "E-mail Address:" with placeholder text "Please enter your name here" and "Please enter your e-mail address here" respectively.
- Three buttons at the bottom: "SUBMIT", "SAVE", and "CANCEL". A red text note next to the "SAVE" button says "Please provide details of the bug you are reporting in the box above."

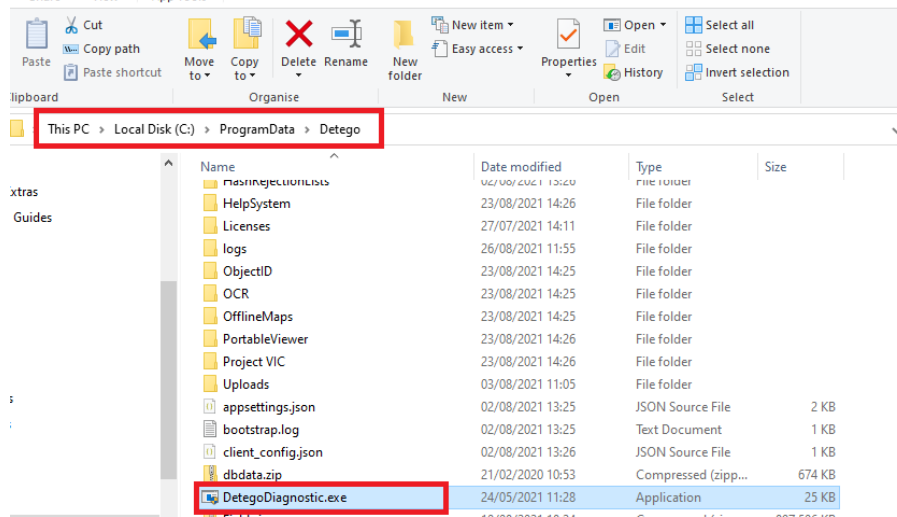
The user can enter a free-text description of the issue and attach files supporting the report (either by selecting them or dragging files in from Windows Explorer). Once a name and email address have been entered, the report can be sent directly to Detego Global (if the machine is online) or saved to a file to be forwarded later.

If you are experiencing any issues with Detego or need assistance, don't hesitate to contact support@detegoglobal.com with your details and diagnostic logs. See below for steps on gathering diagnostic logs to help us diagnose the issue.

- Navigate to the file path: C:\ProgramData\Detego and run the 'DetegoDiagnostic' .exe tool.
 - The 'ProgramData' folder is hidden; enable the 'View hidden items' checkbox from the 'View' menu in File Explorer.

- Once you have run the Diagnostic tool, a .zip file will be placed on your desktop. Send that file to us at the above email address.

Figure 676



8. BIOS KEYS

BRAND	BIOS KEY
Acer	F1, F2, CTRL+ALT+ESC
AST	CTRL+ALT+ESC or CTRL+ALT+DEL
Cannon	F1
Castex	DEL
Compaq	(Red Compaq Logo Screen) F10
CompUSA	DEL
Cybermax	ESC
Dell	DEL
	Dell Dimensions 4100 – 8100 = Tap the F2 key at blue Dell screen
	Dell 400 = F1
	Dell Dimension® = F2 or DEL
	Dell Inspiron® = F2
	Dell Latitude = Fn+F1 (While booted)
	Dell Latitude = F2 (on boot)
	Dell Optiplex = DEL
	Dell Optiplex = F2
	Dell Precision™ = F2
Digital	F2
eMachine	DEL
Enpower (Laptop)	CTRL+ALT+S

BRAND	BIOS KEY
Fujitsu	Press F2 once the Fujitsu logo appears (Lifebook, Esprimo, Amiro, Tablet, DeskPower)
Gateway	F1 or F2
	2000, 1440 = F1
	Gateway 2000 Solo™ = F2
HP (Hewlett-Packard)	F1, F2, DEL or F1 (at blue screen) ESC or F10
HP (Pavilion Notebook)	F2 (inside BIOS) or F10
IBM (Aptiva)	F1
IBM	F1 IBM E-pro Laptop F2 IBM PS/2® CTRL+ALT+INS after
	CTRL+ALT+DEL
IBM Thinkpad (newer) Windows	Programs-Thinkpad CFG
Intel	Tangent DEL
Leading Edge	CTRL+ALT+S
Lenovo	F1 or F2 – Older products may utilise CTRL+ALT+F3, CTRL+ALT+INS or Fn+F1
Micron	F1, F2 or DEL
NEC	F1 or F2
Packard Bell	F1, F2, DEL (After Packard Bell startup screen) F1 or F2
Quantex	DEL key
Samsung	Press F2

BRAND	BIOS KEY
Sony VAIO	(After Sony startup screen) F2 then F1
Sharp	F2 – Some very old Sharps require a Setup Diagnostics Disk to access the BIOS
Shuttle	F2 or DEL on startup
Tiger	DEL
Toshiba	XP Laptops: Drom desktop, click Start > All Programs/ Programs > TOSHIBA Console >TOSHIBA Console
Toshiba Portable PC (Phoenix)	Press the F2 key while the system processes its power on Self-Test (POST)
Toshiba	Rebooting, press ESC and F1 to enter BIOS setup
	335 CDS = ESC
	Toshiba Protégé = ESC
	Toshiba Satellite 205 CDS = F1
	Toshiba Tecra F1 or ESC



DETEGO
GLOBAL

DETEGO GLOBAL

Website: www.detegoglobal.com

Product Enquiries: marketing@detegoglobal.com

Product Support: support@detegoglobal.com