# Reviewing Scan Results

## Introduction

This guide covers how to analyze the findings of a scan.

| This document applies to the following applications | | |
|---|---|---|
| ADFPRO Mobile & Computer Triage | DEI Digital Evidence Investigator | MDI Mobile Device Investigator |

## What are Scan Results?

Scan results are created during the scan of a target device or logical data. They contain records of files and artifacts identified by the Captures for matching precise search criteria.
Scan results can be reviewed by navigating through records, filtering, sorting, tagging, commenting, and creating a report with the relevant information.

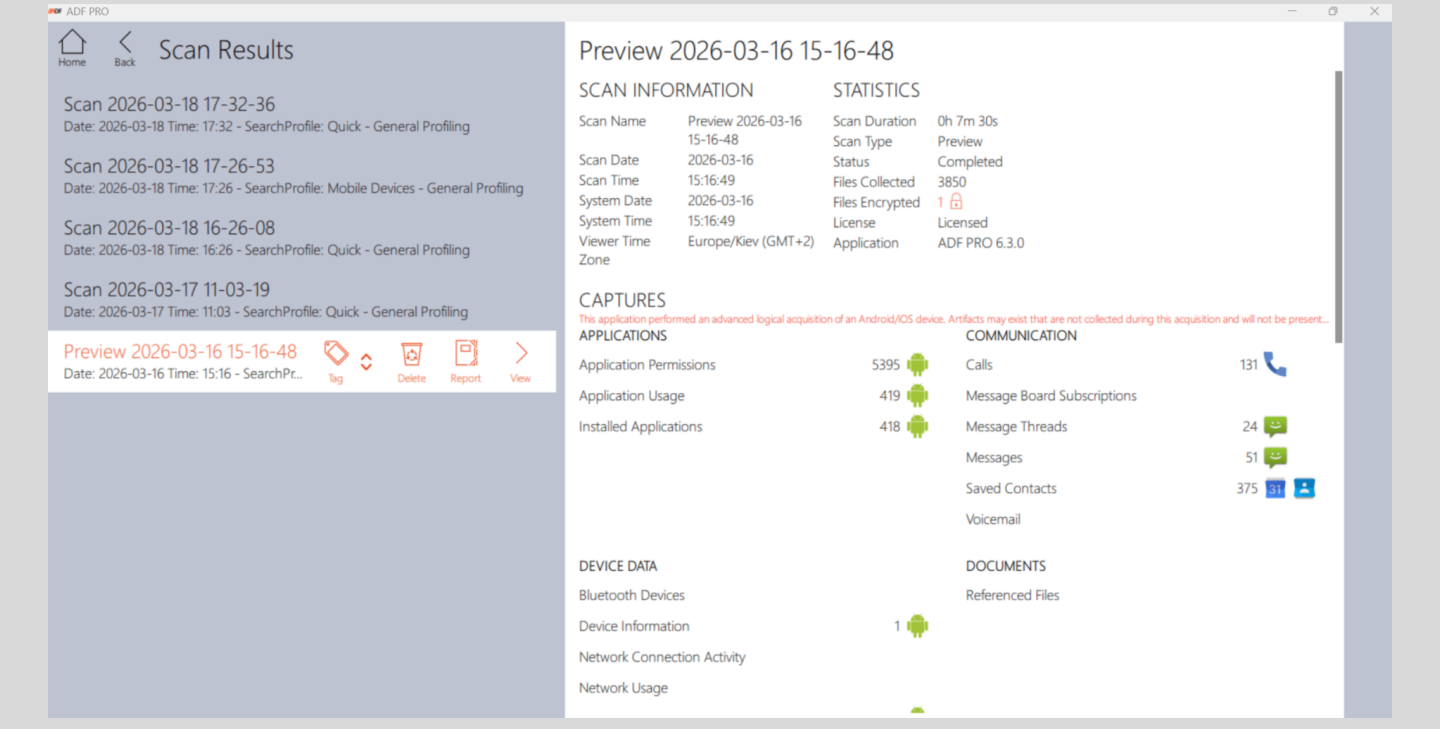
## Reviewing Scan Results

Accessing scan results can be done by

1. Navigating to **Home** > **Review Scan Results**.
2. This page shows the available scan results detected in the default folder (see the data paths) and on any connected Collection Keys.
3. Clicking the **VIEW RESULTS** button during or after a scan.
4. Create a Standalone Viewer report.

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

## Select Scan Result




The scan results are listed on the left-hand side of that screen and sorted from the most recent at the top. Each scan result is identifiable by its scan name, scan date, and Search Profile used. Upon selecting a scan result its summary is shown on the right panel and the following actions are offered:

| | |
|---|---|
|  Tag | To assign or remove a Tag to the scan result. |
|  Delete | To delete the scan result. It is possible to undo this action for 30 seconds.<br>In addition to deleting the scan result, connected mobile device acquisitions can also be deleted at the same time. Note however that a mobile device acquisition created in Preview mode will not be presented and have to be deleted manually. |
|  Backup | To copy the scan result found on a Collection Key to the default location (see the data paths). |
|  | To open the scan result on the report creation screen. |

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

| Report | |
|---|---|
|  View | To view the scan result. Double-clicking on the scan result also selects this action. |

On the right-hand side of the screen the summary of the scan result is displayed.

## Assign Tag to Scan Result

To assign a tag to a scan result, select the Tag icon action button. Choose the relevant tag from the dropdown list. Once selected, the chosen tag's color will be displayed on the far left-hand side of the scan result, providing a visual indicator of the assigned tag.

To remove a tag from a scan result, select the Tag icon again. Select the transparent or clear tag option. Upon selection, the assigned tag will be removed from the result, and the tag color indicator will disappear from the left-hand side.

# Summary View

The Summary view comprises five main sections: Scan Information, Search Profile, Statistics, Captures and Target Devices.

The Scan Information section details the Scan Name, Scan Date and Scan Time, the System Date and System Time and the Viewer Time Zone (see how the Viewer Time Zone is established here).

The Search Profile section shows the Search Profile used to generate the scan result and any associated Notes on the Search Profile.

The Statistics section shows the Scan Duration, the Scan Type (Boot/Live/Desktop/Preview), the Status, the Stealth Mode (ADFPRO Mobile & Computer Triage DEI Digital Evidence Investigator), the number of Files Collected, the number of encrypted files, and the application and version number used.

The Tags Statistics are also shown if any exist.

The number of encrypted files represents the number of files that could not be processed by the Captures as they were identified as encrypted. The "Files Encrypted" text is a hyperlink that opens the Files view and shows these encrypted files. These encrypted files are collected when the "Collect protected files encountered by the Captures (max 2GB)" option is selected in the Search Profile (see Creating a New Search Profile in the Setting Up Scans guide).

The scan Status is defined in the table below. Any status other than Completed is shown in red:

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

| Scan Status | Explanation | Scan Log Message (in scan log) |
|---|---|---|
| Completed | Scan completed successfully | NA |
| In Progress | Scan is in progress | NA |
| Interrupted | User puts the scan on hold | Scan was paused by the user. |
| Crashed | Application crashed during the scan | NA |
| Incomplete | Not all files can be cached | File system metadata is corrupted for SRCX/PARTN. Setting scan status as Incomplete as not all files could be cached. |
| Out of Storage | No space left on destination drive in Desktop scan | Destination drive ran out of storage space. |
| Incomplete | No memory left | System ran out of memory so the scan cannot complete. |
| Incomplete | Target device no longer accessible | Target device no longer accessible so the scan cannot complete. |

The Captures section lists the Captures used in the Search Profile and alongside each capture the number of records found. Each of the Capture names are hyperlinks and by clicking them the individual Capture results are displayed. Captures where no results were identified during the scan will not have a result number next to them. Capture names are appended with the "incomplete" suffix if the scan finishes with a status other than 'In Progress' or "Completed". Detailed information is available in the tooltip on hover.



To view the description of an artifact capture, hover the mouse over its name.

The Target Devices section shows the details of the target devices that were scanned. It contains the following properties per target:

- For a drive
  - Name
  - Label (SrcN by default or defined prior to the scan)
  - Serial number
  - Bus type
  - Sector size
  - Size
  - Partition table type
    - Partition details:
    - Mount letter name
    - Size
    - File system

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

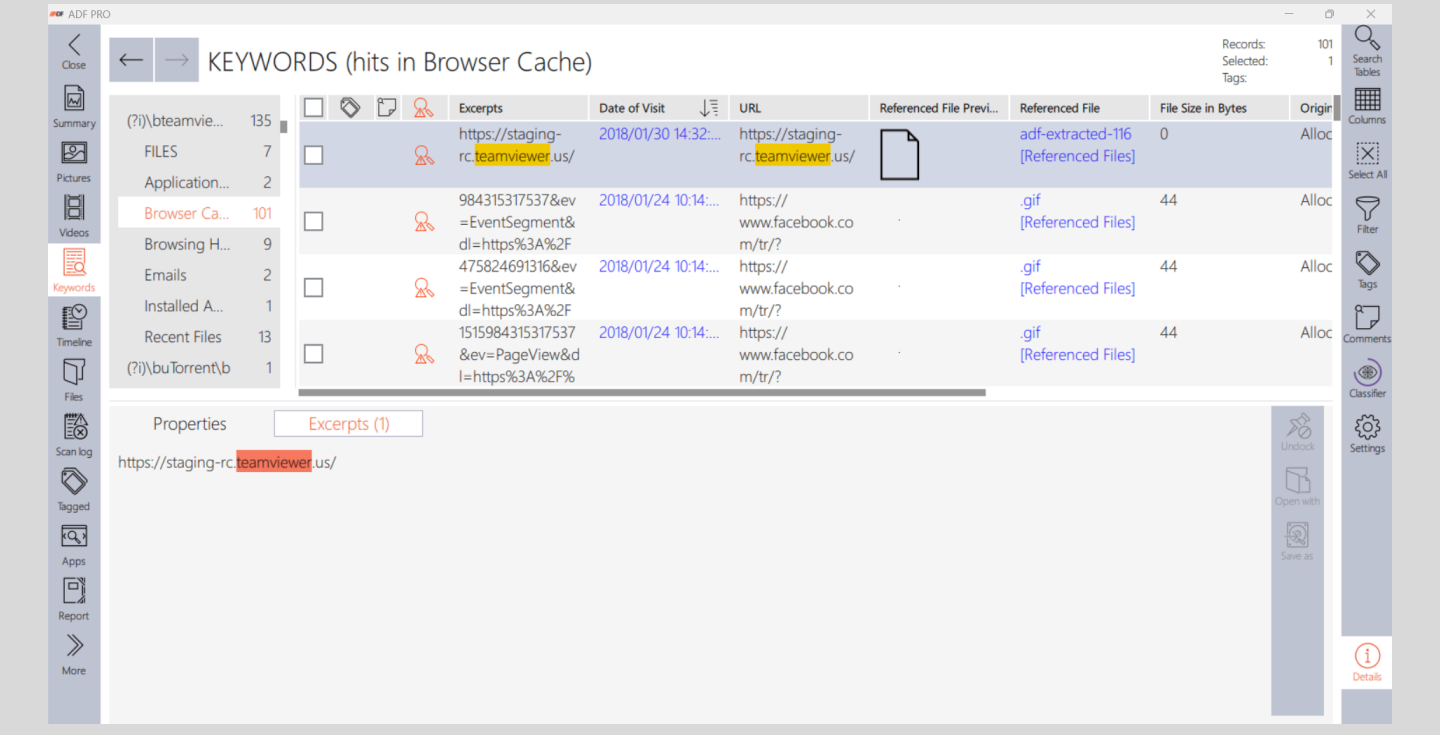
        - Time Zone (if the partition contains an Operating System with time zone information)
- For a drive image
    - Path to the drive image file
- For a folder
    - Path to the folder
- For an MTP device (ADFPRO Mobile & Computer Triage MDI Mobile Device Investigator)
    - Name
- For a mobile device acquisition (ADFPRO Mobile & Computer Triage MDI Mobile Device Investigator)
    - Name
    - Label
    - Serial Number
    - Time Zone
    - Acquisition Duration
    - Acquisition Status (see table below)
    - Acquisition Type (possible values are: Shared Data, Preview Data, Backup Protocol, Acquisition Agent)
- For a mobile device (ADFPRO Mobile & Computer Triage MDI Mobile Device Investigator)
    - Name
    - Label
    - Serial Number
    - Time Zone

| Acquisition Status | Explanation |
|---|---|
| Completed | Acquisition completed successfully |
| Incomplete (missing method) | The acquisition is incomplete because one of the data acquisition methods did not run. The missing method is listed in parenthesis as one of: Shared Data, Backup Protocol, Acquisition Agent. More details on these acquisition methods can be found in the Acquiring an iOS, Android or ChromeOS Device guide for Android and for iOS. |
| Incomplete | The acquisition is incomplete (probably due to disconnection) but the data can still be scanned. |

# Screens Layouts and Controls

The main screen is composed of the following areas: view title panel, forward/backward navigation toolbar, filter summary panel, statistics panel, left-hand side navigation toolbar, records panel, records list panel, details panel, details panel toolbar, and more.

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.




## Backward and Forward Navigation Toolbar

At the top left-hand side of the screen are the Backward and Forward buttons. These allow navigation backwards and forwards in the view history.

| | |
|---|---|
| ← | To move backward in the view history. Hold to see history. |
| → | To move forward in the view history. Hold to see history. |

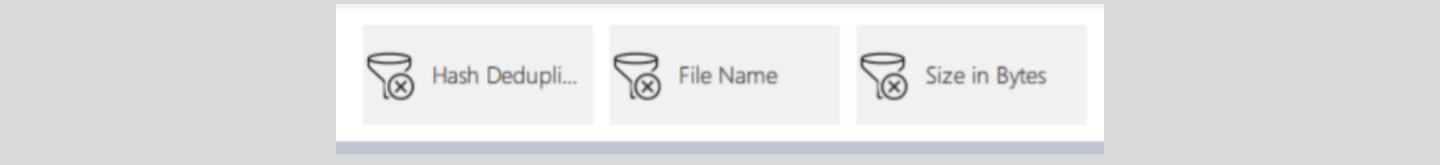
## View Title Panel

This panel shows the name of the view being displayed.

## Filter Summary Panel

When filters are applied, the name of the filtered column is displayed in that panel. It is also possible to remove that filter by clicking on the funnel icon.

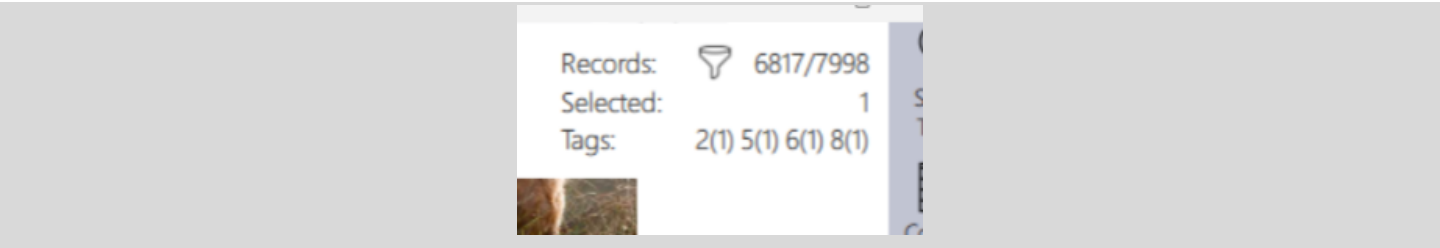
Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.




## Statistics Panel

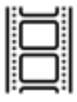
The stats panel shows the following information:

- The number of records displayed out of the total number of records available in that view
- The number of records selected
- The tags applied in this view indicated as tag_number(number_of_records_tagged). For example, if 3 records are tagged with tag #1 and 7 records are tagged with tag #5 then the following is displayed: 1(3) 5(7)




## Navigation Toolbar

Located vertically on the left-hand side of the screen is the navigation toolbar. This toolbar will allow navigation through the results. The following buttons are located on this toolbar:

| | |
|---|---|
|  Close | To close the currently viewed scan result and returns to the previous screen. |
|  Summary | To access the Summary view. |
|  Pictures | To access the Pictures view. This shows a gallery view of all pictures identified by the Captures in the Search Profile. |
|  Videos | To access the Videos view where it is also possible to access the frame view and video player functionality. |

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

| | |
|---|---|
|  Keywords | To access the Keywords view showing keyword hits from keyword searches. |
|  Timeline | To access the Timeline view showing a listing of all artifact and file Capture records in a single timeline. |
|  Files | To access the Files view which lists all files and folders upon the target devices. |
|  Scan log | To access the log of encountered protected files and parsing or scanning events. |
|  Tagged | To access the Tagged View which lists all tagged records. |
|  Apps | To access the Applications cross-capture view. |
|  Report | To access the Report creation view. |
|  More | To open the Navigation panel to access individual Capture results. |

## Navigation Panel

Pressing the More button on the navigation toolbar opens the navigation panel. It shows at a glance all the Captures and their results which are hyperlinked.

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.




## Function Toolbar

A function toolbar is located vertically on the right-hand side of the screen. This toolbar is context specific and will adapt depending on what is being viewed.

| | |
|---|---|
|  Quit | To close the application immediately. |
|  Search Tables | To search the scan result tables for specific keywords. |
|  Columns | To show, hide or reorder columns from the view.<br>To adjust the sort order of displayed results.<br>Changes made to columns display also modify columns displayed within the reports. |

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

| | |
|---|---|
|  Select/Deselect All | To select (check) or deselect (uncheck) all the records within the current view. |
|  Filter | To filter out some records based on their property values. |
|  Zoom | To resize the picture thumbnails. |
|  Tags | To apply tags for selected record(s) in the current view. Renaming of Tags is available here. |
|  Comments | To apply a comment to the selected record(s) in the current view. |
|  Classifier | To display post-scan processing tasks progress. These tasks include the visual classification of pictures, videos, and entity extraction (with add-on).<br>To pause and resume these post-scan tasks.<br>To access Pictures or Videos views filtered by a visual class once the classification is finished or paused. |
|  Settings | To apply settings preferences. |
|  Folder Tree | To toggle the path filter displayed as a hierarchical view of folders.<br>Only visible in the Files view. |
|  Details | To toggle the display of the Details panel which provides further information and functionality for the selected record. |

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

## Details Panel

The details panel provides further information for individual file or artifact records.




The options are displayed in a series of horizontal tabs. Further functionality is accessible via a toolbar displayed on the right-hand side of the details panel. The following table lists the options available in the details panel:

| Option | Function |
|---|---|
| Properties | Individual properties of the selected record. |
| Metadata | Metadata extracted from the selected file. |
| Pages | Displays the individual pages that were collected while performing a series of screenshots with auto scroll on a mobile device ( ADFPRO Mobile & Computer Triage MDI Mobile Device Investigator ). |
| Excerpts | Displays up to 1000 keyword hits highlighted in yellow with surrounding text visible. The instances of the selected keyword are highlighted in red. |
| Frames | Displays up to 50 frames taken at regular intervals from a video file. |
| Preview | Pictures are viewable in this pane at their actual size.<br>Videos are playable via an internal player subject to locally installed codecs.<br>Documents and other files may be viewed by clicking the Undock button on the toolbar.<br>Multi-page screenshots are displayed alongside the extracted text.<br>Blurred previews resulting from sanitized hash matches can be unblurred temporarily from this tab. |
| Duplicates | Displays a list of duplicate files.<br>Duplicate files are identified based on the hash value of their content only. |

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

| | |
|---|---|
| Geolocation Data | Displays geolocation data extracted from the selected record, including latitude, longitude, altitude, absolute altitude, latitude and longitude accuracy, and timestamp, if available. |
| OCR Text | Displays the text extracted from images as a result of the Screen Recordings and Screenshots capture. |
| Participants/Recipients | Displays the complete list of participants for Message Threads capture or recipients for Messages, Emails or Calls captures. |
| Message/Email/Note Text | Displays the full text if it does not fit in the Properties tab for any of the following captures: Messages, Email, or Notes. |
| Associated Folders | Displays the complete list of the Associated Folders for the Installed Applications capture. |

## Details Panel Function Toolbar

On the right-hand side of the Details panel is the functional toolbar.

| | |
|---|---|
|  Undock | To undock the Preview or Frames window. |
|  Open with | To open the file with an external application. |
|  Save as | To save the original file to a chosen location. |
|  Zoom | To resize the frames of the videos or pages that were collected while performing a series of screenshots with auto scroll on a mobile device ( ADFPRO Mobile & Computer Triage MDI Mobile Device Investigator ). |
|  Save HTML | To save the HTML conversion of the original file (so it can be viewed with a web browser instead of the original file's native application) |

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

| | |
|---|---|
|  Search | To search the HTML conversion of the original file for specific keywords. |

## Table Controls

When displaying records in a table it is possible to perform the following operations on the table and columns:

| | |
|---|---|
|  Move | To move a column left or right.<br>Accessible in the Column panel of the functional toolbar.<br>Accessible by clicking and dragging the column header. |
|  Sort ascending | To sort the records in ascending order.<br>Accessible in the Column panel of the functional toolbar.<br>Accessible by clicking on the column header. |
|  Sort descending | To sort the records in descending order.<br>Accessible in the Column panel of the functional toolbar.<br>Accessible by clicking on the column header. |
|  Resize | To resize the column width.<br>Click and drag in-between two column headers. |
|  Show/Hide | To show or hide a column.<br>Accessible in the Column panel of the functional toolbar.<br>Not all columns are displayed by default but they are all accessible in the Column panel. |



For each view, the visible columns, their position, and sort order is maintained when creating a report. Hiding columns such as the Preview column can help sanitize a report.

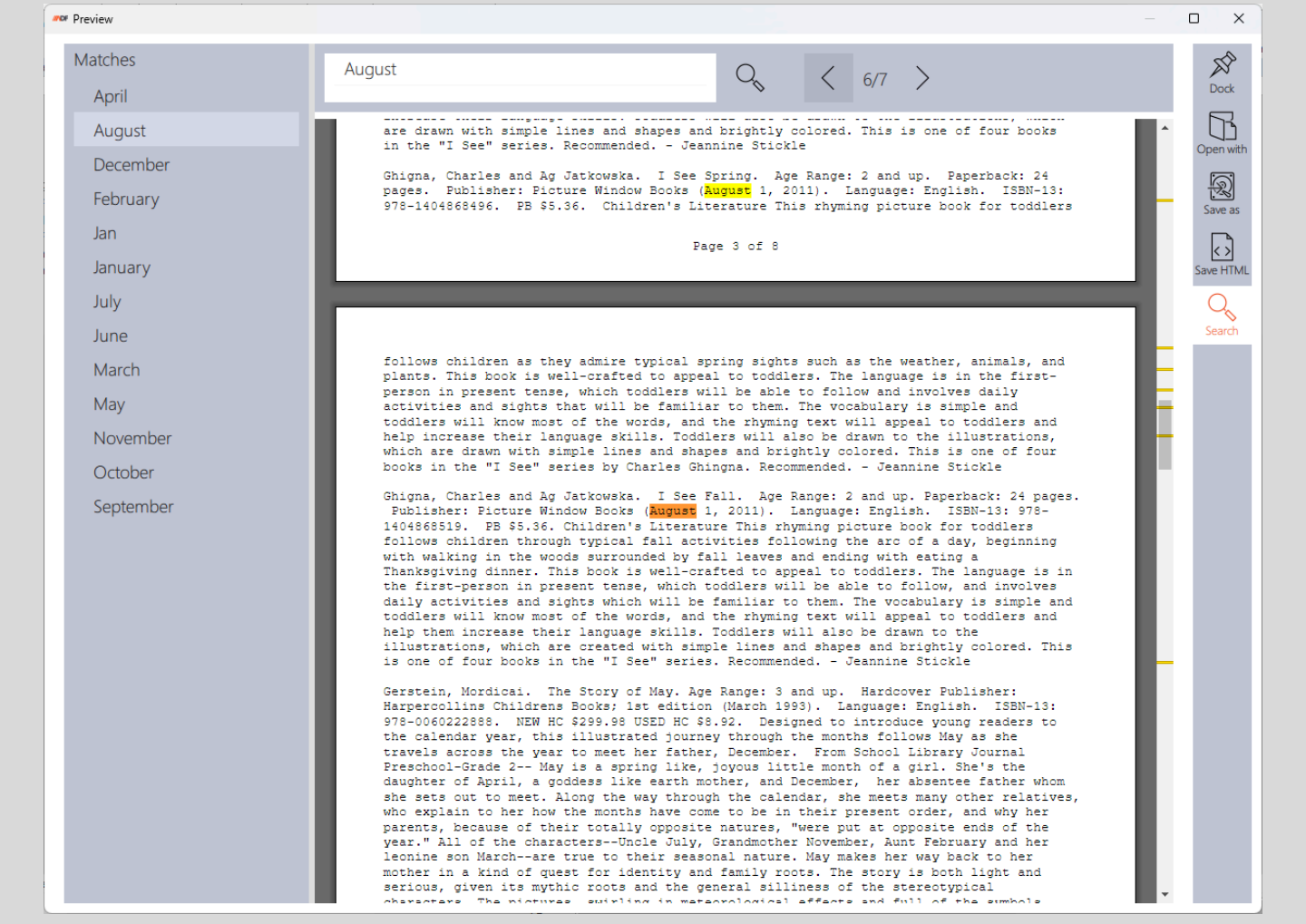
## Undocked Preview Window

The Preview tab in the details pane shows a preview of pictures and other files. On occasion it is not possible to display the file within the details pane, a warning message of “Please undock to view content” will be displayed in such cases. Clicking on the Undock button will open a Preview window.

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

Matched keywords will be shown in the Keywords panel on the left-hand side. This panel lists all keywords used across captures, with those that have at least one match appearing first in alphabetical order. If a keyword has an Expression Name, it will be displayed instead of the search expression to improve clarity.

Selecting a keyword will insert it into the Search bar at the top of the Preview window. Use the navigation arrows in the search bar to move between matches highlighted in the document.




On the right-hand side of the Preview window is the functional toolbar.

| | |
|---|---|
|  Dock | To dock the Preview window |
|  Open with | To open the file with an external application |

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

| | |
|---|---|
|  Save as | To save the file to a chosen location |
|  Save HTML | To save the HTML conversion of the original file (so it can be viewed with a web browser instead of the original file's native application) |
|  Print | To print the contents of the Preview window |
|  Search | To search the HTML conversion of the original file for specific keywords. |

# Analyzing Scan Results

## Record Selection and Navigation

There are several options for selecting records to get more details or assigning tags and comments.

| Action | Method |
|---|---|
| Select one record. | Mouse left click or touch screen tap. |
| Select all the records. | Keyboard Ctrl + A. |
| Select the record with the focus. | Keyboard Spacebar. |
| Select multiple records. | Select the first record then Shift+mouse left click on the last record. |
| Select all the fully visible records. | Keyboard + (Plus). |
| Deselect all the fully visible records. | Keyboard - (Minus). |
| View the next page of records. | Keyboard . (dot) on the number keypad. |
| View the previous page of records. | Keyboard * (star) on the number keypad. |

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

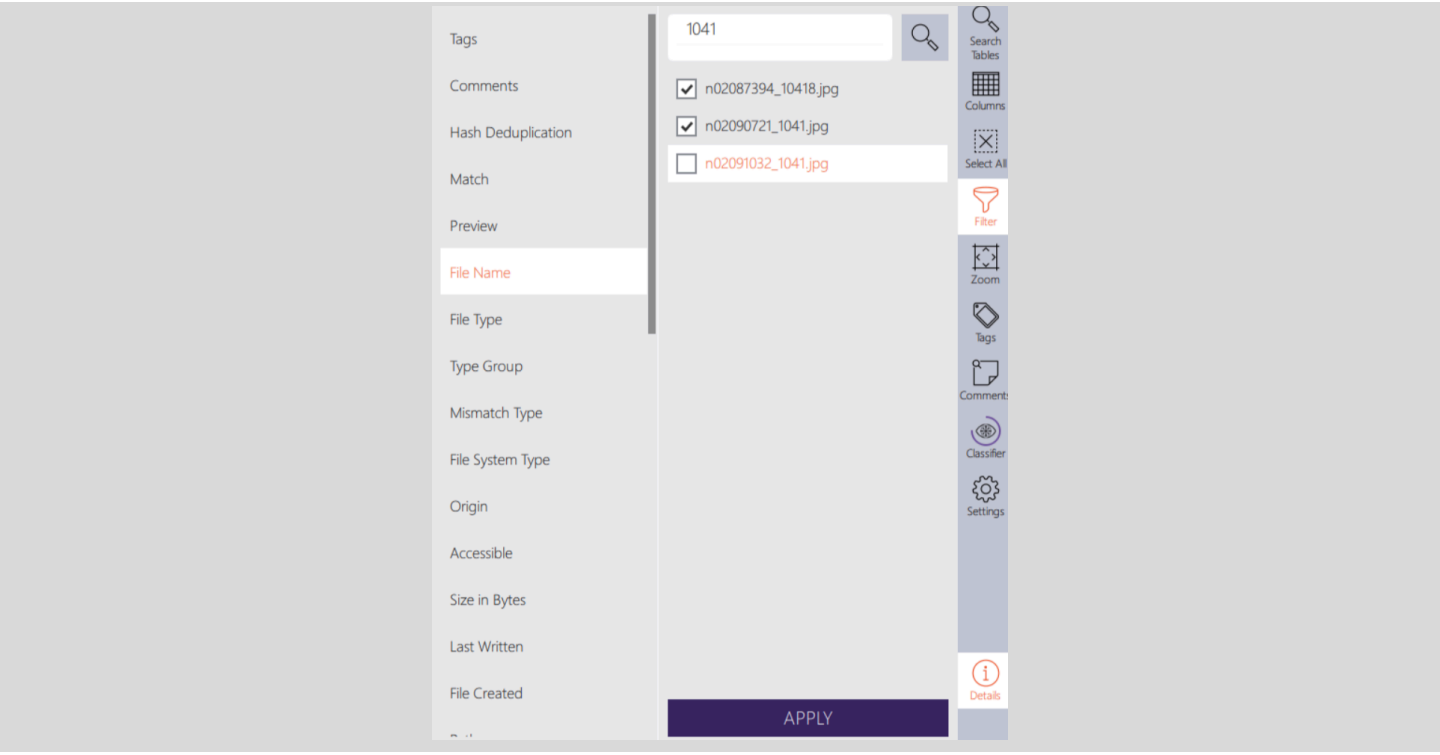
| | |
|---|---|
| Select a nearby record. | Keyboard arrow up, down, left, right. |

## Filtering

Filtering is achieved by selecting the Filter button on the function toolbar. This will open the filter panel and present filters for the current view. It is possible to use multiple filters and the column values are adjusted after each filter is applied. After selecting each filter click the APPLY button on the bottom of the Filter panel. To remove the filter, click the funnel icon on the filter above the table view or click the funnel icon next to the filter in the filter pane. Each table view will have its own set of filters depending on the type of records displayed.

Filters vary depending on the column type.

- Date/time can be filtered by defining a date/time range. The timestamps are adjusted to the Viewer Timezone.
- Numbers can be filtered by defining a range. Some columns offer predefined values (e.g. Photo Probability).
- Paths can be filtered by using the path tree view. Note that multiple paths can be selected.
- Visual classes can be filtered using a confidence range for each class. Note that multiple classes can be selected.
- Capture names can be filtered using a tree view presenting the Captures and their groups.
- Textual information can be filtered with the following methods:
    - Selecting values in the list. Note that only the first 100 values are displayed in the list. It is possible to reduce the number of values in the list by typing a string in the edit box.
    - It is also possible to avoid selecting values from the list and simply clicking on the Magnifier icon to filter using the text entered.




Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

Active filters are shown next to the column name that has been filtered (represented by the icon) and in the top filter summary panel. The filter can be removed by clicking on that icon.

## Sorting

It is possible to sort the records when looking at a table or in a thumbnail gallery view. The sorting capabilities are described in the Table Control section.

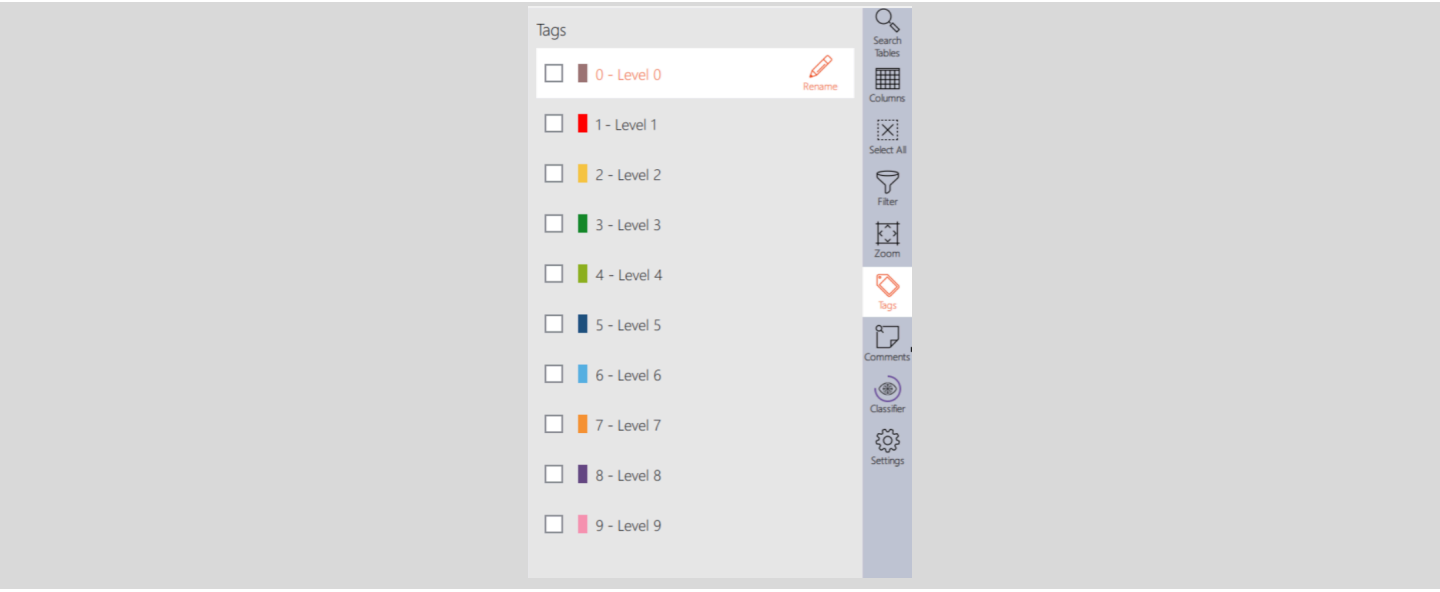
The sort order of each view is maintained when creating a report.

## Tagging

It is possible to assign one or more tags to a record. Tags are useful to help records stand out and to select what to include in a report.

Tags may also be assigned automatically during a scan to records that match keywords or hash values. Records that have been tagged automatically have their Auto-Tagged property set to true. This property is reset to false if other tags are applied or removed from these records.

The Tags panel, accessible from the function toolbar, presents the 10 available tags, each with a unique name and color.




The default tags are named Level 0 through Level 9 and can be renamed in the Settings screen or by selecting Rename in the Tags panel function. Tags renamed in the Tags panel will not affect other scan results.

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

| Action | Method |
| --- | --- |
| Tag one or more records. | After selecting the record(s):<br>● Open the Tags panel and check the appropriate tag checkboxes.<br>● Or, press the number key 0-9 as appropriate. Note that after assigning a tag to one record, the next record is automatically selected.<br><br>In a table view, tags are visible in the Tag column (  ) and represented by a rectangle.<br>In a gallery view, tags are represented by a rectangle at the bottom of the thumbnail (for thumbnails greater than 96 pixels).<br><br>By default, selected checkboxes remain checked after assigning a tag. Select the **Setting** icon in the **Function Toolbar** to modify this behavior. |
| Untag one or more records. | After selecting the record(s):<br>● Open the Tags panel and uncheck the appropriate tag checkboxes.<br>● Or, press the number key 0-9 corresponding to the tag to be removed. |



Tags are a useful way to select the content that later gets exported into a report.

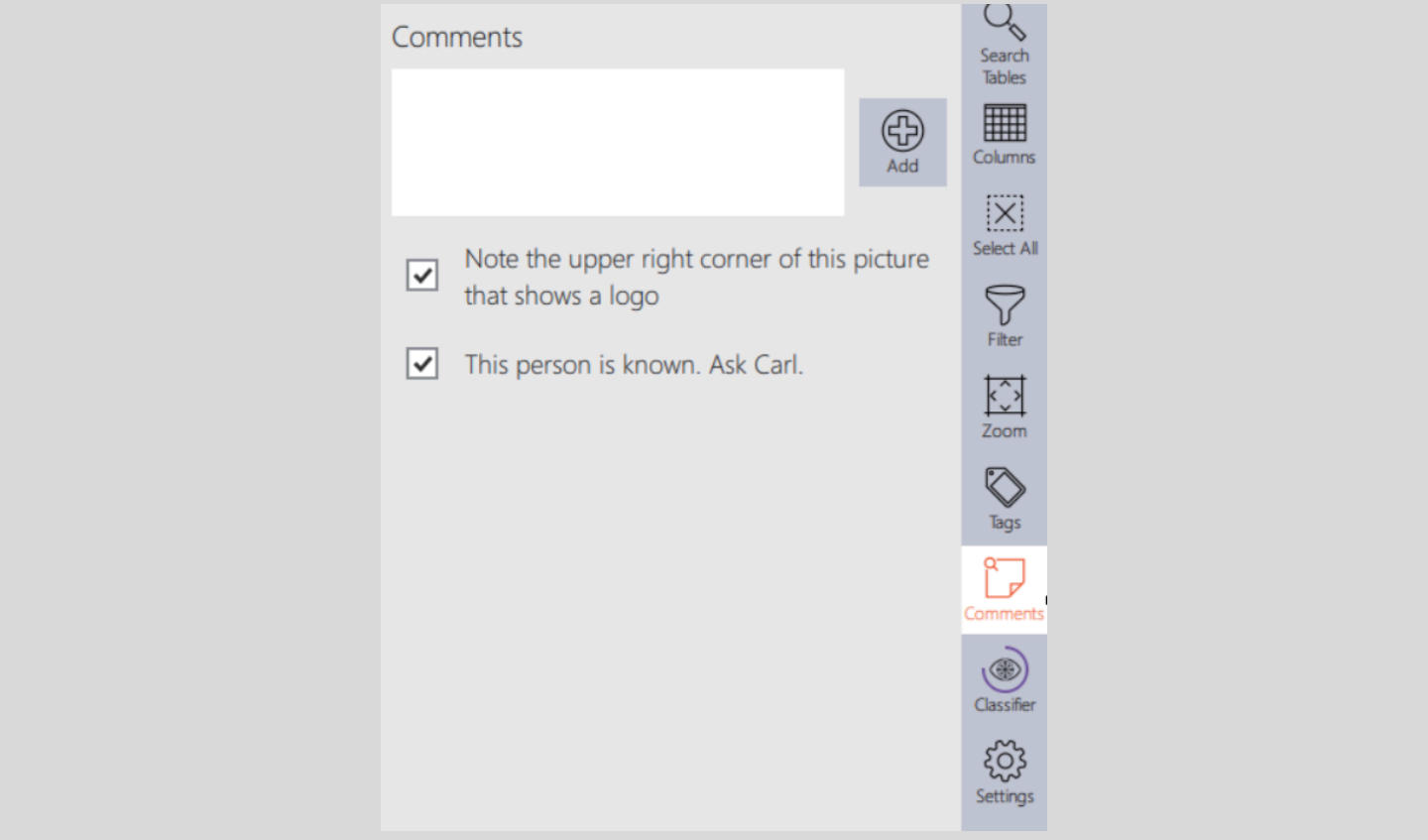
## Commenting

It is possible to assign one or more comments to a record. Comments are useful to annotate and group records and they are included in a report.

Comments may also be assigned automatically during a scan to records that match keywords or hash values.

The Comments panel, accessible from the function toolbar, presents the available comments and makes it possible to create new comments.

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.




The default tags are named Level 0 through Level 9 and can be renamed in the Settings screen or by selecting Rename in the Tags panel function. Tags renamed in the Tags panel will not affect other scan results.

| Action | Method |
|---|---|
| Assign a new comment to one or more records. | After selecting the record(s):<br>• Open the Comments panel and type the new comment in the edit box, then click the Add button.<br><br>In a table view, comments are visible in the Comment column ( ) and represented by a similar icon.<br>In a gallery view, comments are represented by the Comment icon on the right-hand side of the thumbnail (for thumbnails greater than 96 pixels). |
| Assign one or more existing comments to one or more records. | After selecting the record(s):<br>• Open the Comments panel and check the existing comment checkboxes in the list. |
| Edit an existing comment. | Open the Comments panel and mouse-over the comment to see the Edit button. After clicking this button, the comment can be edited. Modification to a comment affects all the records associated with it. |

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

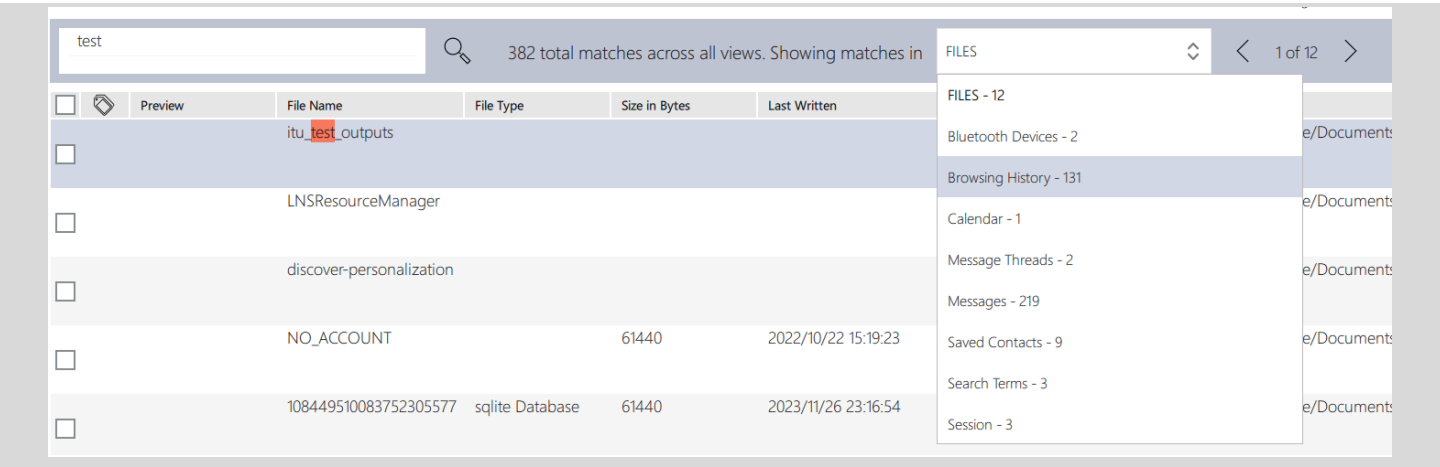
| | |
|---|---|
| Delete an existing comment. | Open the Comments panel and mouse-over the comment to see the Delete button. After clicking this button, the comment is deleted and no longer associated with any records. |
| Unassign a comment to one or more records. | After selecting the record(s):<br>● Open the Comments panel and uncheck the appropriate comment checkboxes. |



Comments are a useful way to annotate important records and they appear in a report.

## Searching Scan Results

A keyword search can be performed within the scan result data (excluding the original file contents). To start, click the Search Tables button in the function toolbar. After the search completes, the total number of matches across all views is displayed, along with the matches for the currently selected record type shown in the dropdown menu.
Use the dropdown to switch between record types (for example Files, Browser Cache, or Messages) to view their respective matches.
Use the left and right arrow buttons to navigate between individual keyword hits.






The Search Tables function is only available after the indexing of the scan result textual content is complete.

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

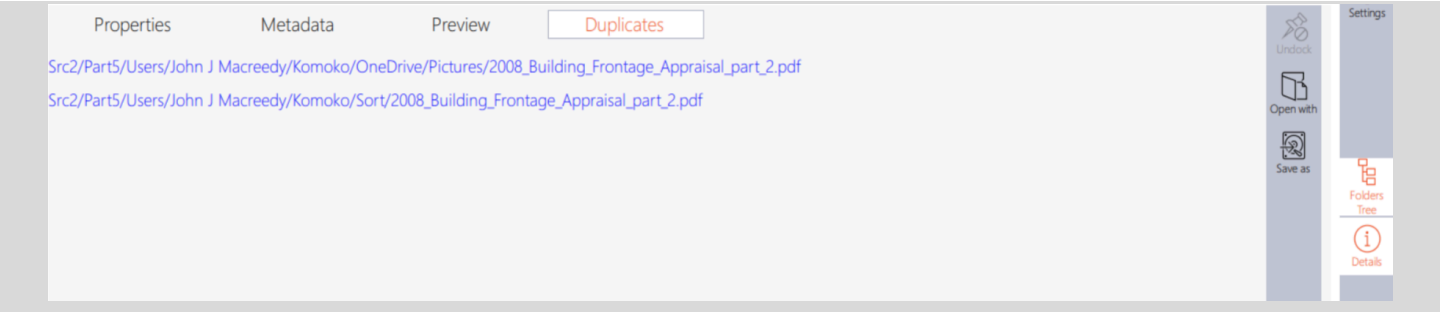
| Action | Method |
| --- | --- |
| Execute a keyword search | Open the Search Tables panel from the function toolbar and type the keyword in the edit box.<br><br>The keyword entered can only be matched against the beginning of words and it is case insensitive.<br><br>Use spaces in place of unsupported characters. For example, when searching for "myfile.png" type "myfile png" instead. |
| Search for dates | To conduct a search for dates, enter the date in the format yyyy/mm/dd where yyyy is the year, mm is the month and dd is the day (e.g. 2014/11/25), any dates matching this will be identified as a search hit. |
| Navigating through the search results | The Search Tables panel shows the total number of matches found. Use the dropdown to select an artifact type and view its specific match count. The panel also displays the current match position relative to the total matches in the selected source.<br><br>Use the left ( < ) and right ( > ) arrow buttons to navigate through the results for the selected artifact type.<br><br>The search term will be highlighted in red in the table cells and in the Details panel. Note that keywords highlighted in yellow have been identified by a keyword search Capture as described in the Keywords View paragraph. |

## Deduplicating Files

It is possible to filter out duplicate files. Files are considered duplicate if they have the same hash value and file size. To hide duplicate files, check the Hash Deduplication checkbox in the Filter panel. This feature is available whenever file records are displayed.

Files that have duplicates can be identified by the Duplicates tab in the Details panel, or by the duplicates icon ( ) overlaid on top of a thumbnail.
In the Details panel, the Duplicates tab shows the paths of the other duplicates. These paths are hyperlinks that point to the Files view.

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.




Tagging a duplicate file tags all the duplicates. The same is true when assigning a comment.

## Referenced Files

When an artifact record references a file found on the target file systems, a link is established between the two. We refer to these files as referenced files. A thumbnail preview of the referenced file(s) is provided, and hovering the mouse over it reveals the name of the referenced file. A hyperlink makes it possible to navigate from the artifact record to the referenced file(s). Another hyperlink, called Linked Artifacts, exists between the referenced file and their artifact record(s).

The following artifact Capture results contain records that may reference files on the target device(s) or files embedded within files on the target device(s).

| Artifact Capture | Notes |
|---|---|
| Browser Cache | This artifact Capture extracts cached files from containers used by the Google Chrome, Safari, Edge, Opera and Firefox browsers. The extracted cached files are listed within the Files view and shown as embedded files. We also treat these files as referenced files. These referenced files are accessible by a hyperlink in the Referenced File column. Hyperlinks will exist to the Files view record for the cached file and to any file Captures that have collected the file concerned. |
| Cloud Files | This artifact capture collects records of files on target devices which exist(ed) on the filesystem that potentially have online backups via cloud storage solutions. The files available on the filesystem are treated as referenced files. These referenced files are accessible by a hyperlink in the Original File column. Hyperlinks will exist to the Files view record for the attached file and to any file Captures that have collected the file concerned. The Original File column can also contain details of other Captures that reference the file. |
| Download History | This artifact Capture recovers information relating to downloaded files. Downloaded files that can be located upon the target device(s) are treated as referenced files and are accessible by a hyperlink in the File Name column. Hyperlinks will exist to the Files view |

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

| | |
|---|---|
| | record for the downloaded file and to any file Captures that have collected the file concerned. |
| Emails | This artifact Capture recovers email client messages. These messages may have associated attachments. These attachments are treated as referenced files. These referenced files are accessible by a hyperlink in the Attachment Names column. Hyperlinks will exist to the Files view record for the attached file and to any file Captures that have collected the file concerned. The Attachment Names column can also contain details of other Captures that reference the file. |
| Messages | This artifact Capture recovers messaging client messages. These messages may have associated attachments. These attachments are treated as referenced files. These referenced files are accessible by a hyperlink in the Attachment Name column. Hyperlinks will exist to the Files view record for the attached file and to any file Captures that have collected the file concerned. The Attachment Name column can also contain details of other Captures that reference the file. |
| Notes | This artifact capture collects a list of notes from note taking applications. These notes may have associated attachments. These attachments are treated as referenced files. These referenced files are accessible by a hyperlink in the Attachment Names column. Hyperlinks will exist to the Files view record for the attached file and to any file Captures that have collected the file concerned. The Attachment Names column can also contain details of other Captures that reference the file. |
| Notification | This artifact capture collects a list of recent notifications received on target devices. These notifications may have associated attachments. These attachments are treated as referenced files. These referenced files are accessible by a hyperlink in the Attachments column. Hyperlinks will exist to the Files view record for the attached file and to any file Captures that have collected the file concerned. The Attachments column can also contain details of other Captures that reference the file. |
| P2P Files Shared or Downloaded | This artifact Capture recovers information relating to files downloaded or shared by P2P applications. If these files can be located upon the target device(s) they are treated as referenced files and are accessible by a hyperlink in the Candidate column to the relevant file record in the Files view. The Candidate column can also contain details of other Captures that reference the file. |
| Recent Files | This artifact Capture identifies recently accessed files. Recently accessed files that can be located upon the target device(s) are treated as referenced files and are accessible by a hyperlink in the Candidate column to the relevant file record in the Files view. Candidate files are identified by matching their File Name and File Path with the information within the artifact Capture record. |
| Reminder | This artifact capture collects a list of reminders from applications. The reminders may have associated attachments. These attachments are treated as referenced files. These referenced files are accessible by a hyperlink in the Attachments column. Hyperlinks will exist to the Files view record for the attached file and to any file Captures that have |

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

| | |
|---|---|
| | collected the file concerned. The Attachments column can also contain details of other Captures that reference the file. |
| Voice Mail | This artifact capture collects information related to voicemails extracted from applications. These mails are saved in audio files, they are treated as referenced files. These referenced files are accessible by a hyperlink in the Referenced File column. Hyperlinks will exist to the Files view record for the attached file and to any file Captures that have collected the file concerned. The Referenced File column can also contain details of other Captures that reference the file. |
| Voice Memo | This artifact capture collects voice memo data saved in voice memo applications. These memos are saved in audio files, they are treated as referenced files. These referenced files are accessible by a hyperlink in the Audio File column. Hyperlinks will exist to the Files view record for the attached file and to any file Captures that have collected the file concerned. The Audio File column can also contain details of other Captures that reference the file. |

## Keyword and Hash Match Indicator

File records that have been identified by a keyword search or a hash value search may be more relevant than the other records because they match a specific search criteria. To help them stand out, the Match indicator (  ) is shown in tables and gallery views.

The Match indicator can also be used to sort and filter records.

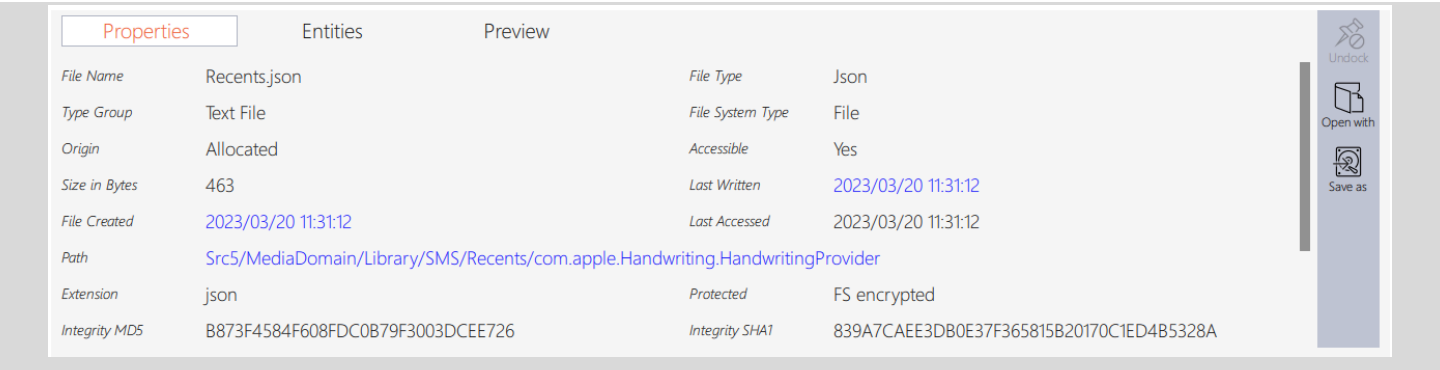
Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

# Entities Property

| This section applies to the following applications | | | | |
|---|---|---|---|---|
| Rosoka Add-on | | | | |

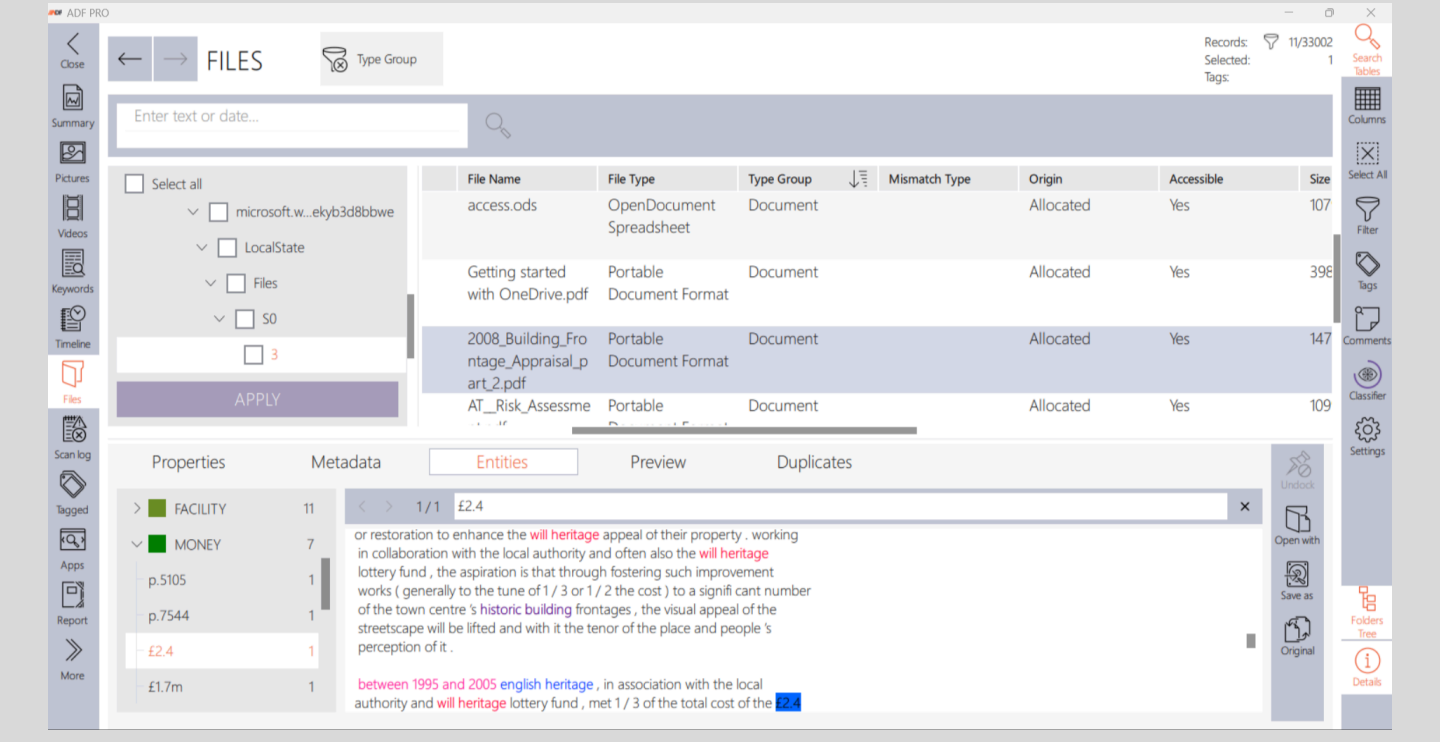
Entities are words of a document that represent a person, a place, an organization, a timestamp, and many more concepts (there are close to 50 different types of entity that can be identified). The Rosoka Add-on can find entities in more than 200 different languages and can translate them back into English.

When entities are identified in a record, the **Entities** record property is populated and the **Entities** tab in the **Details** panel shows them all. The screenshot below shows the **Entities** property:




The screenshot below shows the **Entities** tab of the **Details** panel.

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.




The right-hand side function toolbar of the **Details** panel offers the following actions related to entities extraction:

| | |
|---|---|
|  Gloss | To show the gloss of the document. |
|  Original | To show the plain text version of the document. |

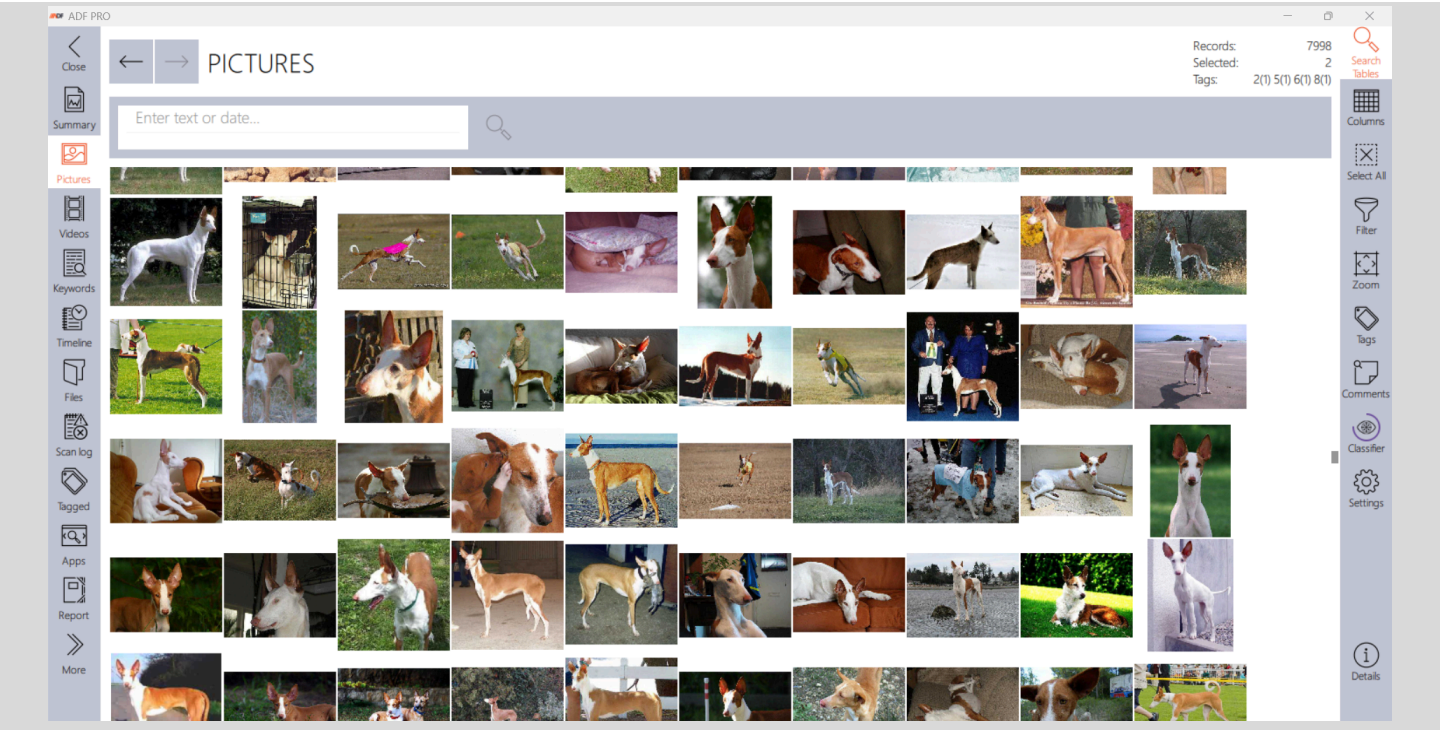
The **Entities** tab shows the following:

- The right-hand side shows a plain text document preview either showing the gloss or the original plain text document. The gloss is the version of the document where the identified entities have been normalized and translated. Each entity is color coded and uses the color of its group.
- The left-hand side shows the entity tree. It lists the entity groups with its color and how many entities are in each group. Expanding a group reveals each entity in this group and how many instances have been found. It is possible to select an entity to see it in the gloss or the original.
- The navigation bar is above the plain text document preview and it appears when an entity is selected.

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

# Pictures View

The Pictures view shows all the pictures processed across all the Captures. They are presented in a gallery of thumbnails that can be resized with the Zoom button in the function toolbar.




## Blurred Pictures

Hash matches can be configured to automatically blur the matching pictures to avoid unnecessary exposure to harmful content. These pictures can still be viewed by selecting the Preview tab of the Details panel and clicking on the SHOW PREVIEW button.

## Visual Indicators

On picture thumbnails larger than or equal to 128 pixels, the following icons may be overlaid:

| | |
|---|---|
|  | The duplicate indicator is shown when the same file (based on its content) was found in multiple locations. |
|  | The Match indicator is shown when the record was matched with a keyword or hash value by a Capture. |

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

| | |
|---|---|
|  | The Comment indicator is shown when a comment is applied to the record. |
|  | The multi-frame indicator is shown when the picture contains more than one frame. Use the Preview tab of the Details panel to view all the frames. |
|  | The geolocation indicator appears when a picture contains location information in its metadata. Use the Geolocation Data tab in the Details panel to view all available details. Hovering over the indicator displays the coordinates in a tooltip. |

## Advanced Picture Analysis

To accelerate the analysis of pictures it is recommended to use the following filters:

### Picture Width and Picture Height

The size of the picture in pixels.

### EXIF Data

The metadata saved by digital cameras in the picture file.

- EXIF Make
- EXIF Model
- EXIF Camera Serial Number
- EXIF Date Time
- EXIF Coordinates

### Photo Probability

Photo Probability filtering is applicable to all pictures within the Picture File Types group. The Photo Probability score indicates how likely it is that the file is a photograph. Files with a score lower than 70% are very unlikely to be a photograph and more likely to be other picture types such as icons and cliparts or similar.
The Pictures and Capture views can be sorted based on the Photo Probability score, allowing non photographic pictures to be quickly removed from the displayed results. High (80% and above), medium (70% and above) and low (50% and above) pre-set options are available.

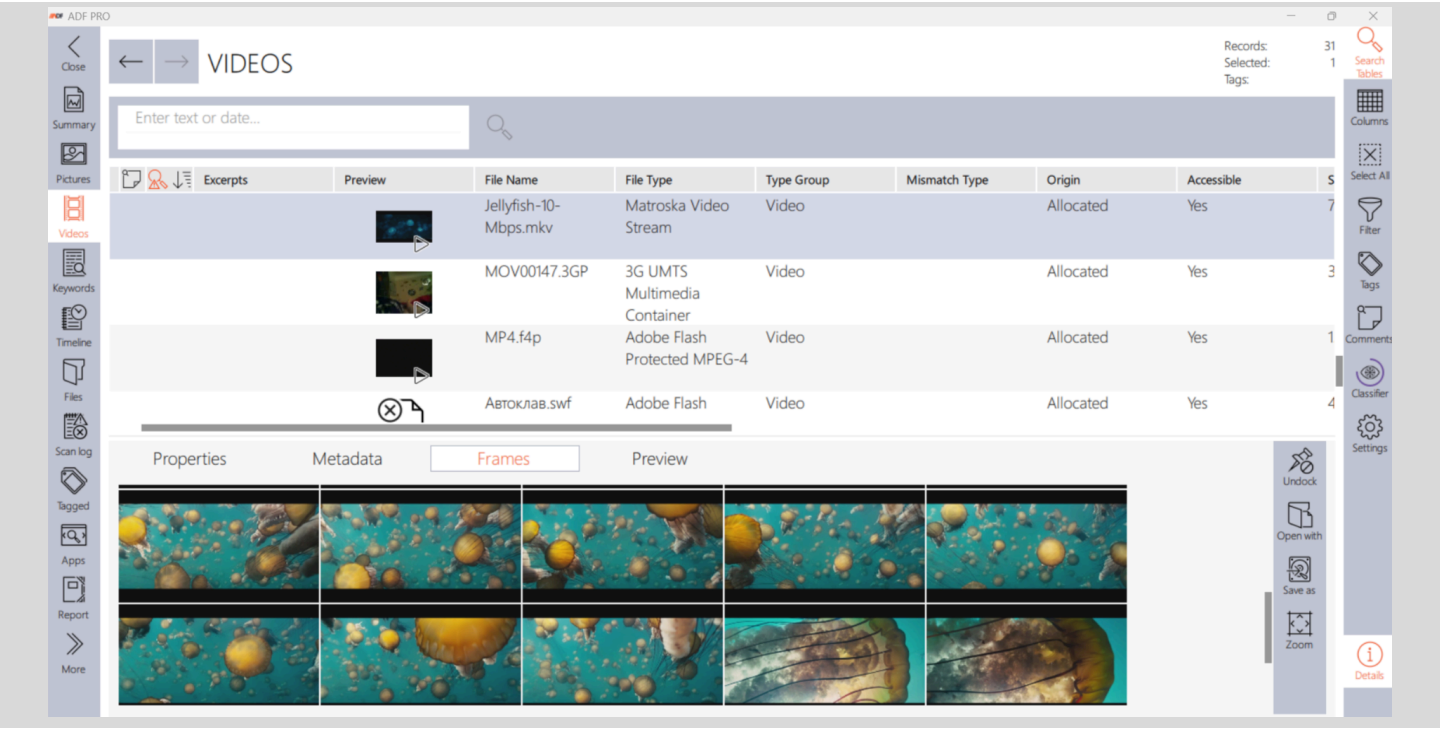
### Picture Visual Class

Use the Visual Class property filter to quickly eliminate pictures that do not represent a group of interest. It is possible to select one or more visual classes and the confidence score range can be adjusted by increments of 5%.

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

# Videos View

The Videos view shows the videos processed across all the Captures. About 50 frames of each video can be viewed in the Frames tab of the Details panel.




## Visual Indicators

On video thumbnails larger than or equal to 128 pixels, the following icons may be overlaid:

| | |
|---|---|
|  | The duplicate indicator is shown when the same file was found in multiple locations. |
|  | The Match indicator is shown when the record was matched with a keyword or hash value by a Capture. |
|  | The Comment indicator is shown when a comment is applied to the record. |

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

| | |
|---|---|
|  | The video indicator is shown when the thumbnail represents a video file. |

## Advanced Video Analysis

To accelerate the analysis of videos it is recommended to use the following techniques:

### Video Duration Filter

Expressed in seconds in the filter. Note that this information is not always extracted.

### Video Frames

Open the Details panel on the Frames tab and use the keyboard arrow down to navigate through the videos one at a time.

### Video Frame Visual Class

Use the Visual Class property filter to quickly eliminate videos that do not represent a group of interest. It is possible to select one or more visual classes and the confidence score range can be adjusted by increments of 5%.

# Visual Classification Processing

Visual classification processes are executed upon a scan commencing and continue in the Viewer. These processes need to be activated in the Search Profile as described in the Creating a New Search Profile section of the Setting Up Scans guide. Progress is shown in the Viewer by the yellow circle around the Classifier icon.




These processes require a lot of CPU power and may slow down the user interface. It is possible to pause their execution in the **Classifier** panel by clicking on the **PAUSE** button. The processes can then be resumed by using the **RESUME** button. If these processes are running and the scan result is closed then they will resume automatically the next time the scan result is opened.

## Picture Classification

The picture classification process classifies each picture into the 11 pre-defined visual classes (Bestiality, Child Abuse, Currency, Others - various innocuous class types, People, Pornography, Portrait, Scanned Doc, Upskirting, Vehicle, and Weapon). Only pictures with a Photo Probability of 70% or more are processed. A picture can be assigned to more than

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

one visual class and a probability score is given for each class. A high probability score indicates that the picture is more likely to belong to that visual class. Assigning a visual class score is not an exact science and some pictures may be misclassified.

### Video Classification

The video classification process classifies each video into the same pre-defined visual classes used to classify pictures (see above). To assign visual classes, each video frame is classified individually, then the video record inherits the highest confidence score from all of its frames.

## Post-Scan Processing

### Entity Extraction

| This section applies to the following applications | | | | |
|---|---|---|---|---|
| Rosoka Add-on  | | | | |

The entity extraction process is executed after the scan completes and continues in the Viewer to shorten the duration of the scans. The entity extraction process needs to be activated in the Search Profile as described in the Creating a New Search Profile section of the Setting Up Scans guide.

With the Rosoka Add-on, entities from texts are identified and translated. Only the following record types are processed:

- Document records
- Communication>Messages
- Communication>Emails (email content)
- Web Browsers>Search Terms

This process is only available in the Desktop application and not during a live or boot scan.

## Keywords View

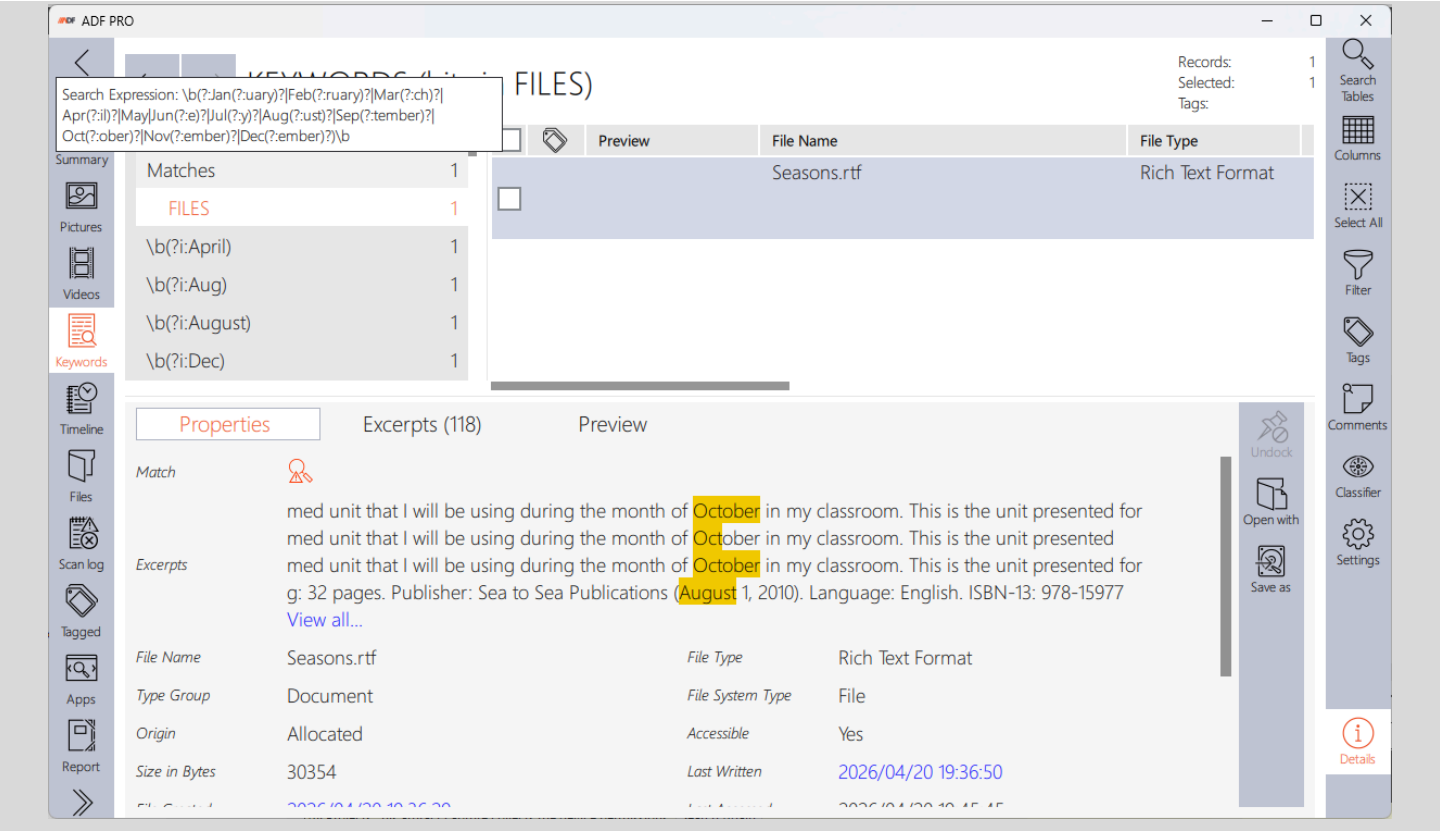
The Keywords view shows all the keyword matches across all Captures. Matching keywords can easily be verified in the Excerpt tab of the Details panel and are highlighted in yellow everywhere they are displayed.

The keyword list panel on the left-hand side shows all the keywords used across all Captures. The keywords with at least one match are listed first and they are listed alphabetically in ascending order. Upon selecting a keyword the sub-list of

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

views is displayed making it possible to navigate faster to a specific view. The number next to the keyword counts the number of records containing that keyword at least once. This number does not count the instances of that keyword.

When viewing keywords that have an Expression Name associated with the search expression, the Keywords panel will display the Expression Name instead of the underlying search expression. This improves readability and helps understand the purpose or intent behind complex search terms such as regular expressions.






In the Excerpt tab of the Details panel, the number in parentheses represents the number of hits for all the keywords found in that record.

The Excerpt tab shows all the keywords found in the selected record, but the selected keyword is highlighted in red as opposed to yellow.

# Timeline View

The Timeline view lists all file and artifact records that have timestamp information. The Timeline view is accessed by clicking the Timeline button on the navigation toolbar. This view is also accessible via timestamp hyperlinks.
It is possible for one record to have multiple activities. For example, each file record has at least the “File created”

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

Here is a description of the Timeline table:

| Name | Description | Visible by Default | Sortable | Filterable |
|---|---|---|---|---|
| Tags | The tags assigned to the record associated with this activity | Y | Y | Y |
| Comments | The comments assigned to the record associated with this activity | Y | Y | Y |
| Match | If the record associated with this activity was matched by keyword or hash value | Y | Y | Y |
| Timestamp | The timestamp of the activity | Y | Y (default ASC) | Y |
| Activity | The name of the activity | Y | | Y |
| Info | Additional information for the activity | Y | | Y |
| Preview | If the activity involves a picture, its preview is displayed | Y | | |
| Principal | If the activity is a communication, its principal is displayed | Y | | Y (merged columns) |
| Recipient | If the activity is a communication, its recipients are displayed | Y | | |
| Virtual Location | The location connected with this activity. It can be a path, a URL, a search engine, etc | Y | | Y |
| Auto-Tagged | If the record associated with this activity was tagged automatically | Y | Y | Y |
| Captures | The name of the Capture that collected the record associated with this activity | Y | | Y |

# Timezone and Timestamps Management

During the course of a scan, many timestamps are collected. They are all saved in the scan results database in UTC so that they can be compared and sorted. Some collected timestamps for which the time zone is unknown, cannot be easily converted to UTC and require identifying their most likely time zone. These timestamps are annotated with (L) when displayed to indicate that they started as local timestamps and that they could be wrong if the likely time zone was incorrectly determined. Determining the most likely time zone is done as follows by searching for time zone information on each target partition that contains an Operating System and using the one from the most recently accessed partition. When no time zone information is found, the most likely time zone is set as follows:

- On a boot scan, UTC is used.
- On a live scan, the target computer time zone is used. If this fails, use UTC.
- On a desktop scan, the running computer time zone is used. If this fails, use UTC.

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

When displaying timestamps, this likely time zone is used to adjust all the timestamps collected in the scan results database. This time zone is referred to as the Viewer Time Zone and it is visible in the Summary view. If no time zone was found, the Viewer Time Zone is set to the viewing workstation.
The time zone can be detected on the following targets:

- Windows: physical OS partition, physical OS encrypted partition (once decrypted), imaged OS partition (DD and E01 formats, time zone is not detected on L01 images)
- macOS (HFS): physical OS partition, physical OS encrypted partition (once decrypted), imaged OS partition (DD and E01 formats)
- macOS (APFS): no timezone detection for now
- Android: mobile device, imaged mobile device (ADF logical acquisition format)
- iOS: mobile device, imaged mobile device (ADF logical acquisition format)

# Files View

The Files view lists all files and folders encountered on the target device(s). The Files view is accessed by clicking the Files button on the navigation toolbar. The Files view is also accessible via hyperlinks when a file is connected with an artifact record (e.g. Download History, Recent Files). File Capture records contain hyperlinks to the file path of the file concerned. When these hyperlinks are clicked the appropriate record is shown within the Files View filtered by the path of the containing folder.

The Files view can be viewed with or without the Folders Tree displayed. This view is toggled by the Folders Tree button on the function toolbar.

Here is a description of the Files table (these columns are similar for all file records):

| Name | Description | Visible by Default | Sortable | Filterable |
|---|---|---|---|---|
| Tags | Tags assigned by the user | Y | Y | Y |
| Comments | Comments assigned by the user | Y | | Y |
| Match | Set to true if that file was matched by hash value or keywords | Y | Y | Y |
| Excerpts | Excerpt from the text around the matching keyword | Y | | |
| Preview | Preview of the picture | Y | Y | Y |
| File Name | File name and extension. Use generated name "adf_embedded_INDEX.ext" when file name is missing inside a container | Y | Y | Y |
| File Type | The name of the file type such as "GNU Zip Archive" | Y | Y | Y |
| Type Group | Should be the name of the file type group such as Archive. | Y | Y | Y |
| Mismatch Type | Contains the file type based on the extension if it doesn't match the header analysis file type | Y | Y | Y |

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

| | | | | |
|---|---|---|---|---|
| File System Type | Possible values: File, Folder, Alternate Data Stream, Symbolic Link, Carved File, Unknown (reparse points or others) | | Y | Y |
| Origin | Possible values are:<br>- Allocated: files that are accessible to the user via the file system<br>- Embedded: files contained within another file (usually archives or cache containers)<br>- Unallocated: files no longer referenced by the file system for which the data can still be found on consecutive sectors<br>- Deleted: files that are still referenced by the file system but marked as deleted and for which the sectors are reusable<br>- Inaccessible: files that are locked and cannot be read | Y | Y | Y |
| Accessible | Possible values are:<br>- True: the content of the file is accessible.<br>- False: the content of the file was inaccessible and only file system metadata were available. | Y | Y | Y |
| Size in Bytes | File size | Y | Y | Y |
| Last Written | Last written timestamp (based on Viewer Time Zone) | Y | Y | Y |
| File Created | File created timestamp (based on Viewer Time Zone) | | Y | Y |
| Last Accessed | Last accessed timestamp (based on Viewer Time Zone) | | | |
| Path | Full path starting with the source (or source label) | Y | Y (default ASC) | Y |
| Extension | File extension | | Y | Y |
| Protected | Possible values: Not protected, FS encrypted, Password protected, Encrypted and password protected | | Y | Y |
| Picture Width | Picture width in pixels | | Y | Y |
| Picture Height | Picture height in pixels | | Y | Y |
| Video Duration | Duration (formatted as #d #h #m #s) | | Y | Y |
| Linked Artifacts | Hyperlink to the artifact records associated with this file | Y | | Y |
| Matching MD5 | MD5 hash value of the file that matches the same hash value from a Capture (displayed in hexadecimal base16) | | | |
| Matching SHA1 | SHA-1 hash value of the original file that matches a hash search Capture (displayed in hexadecimal base16) | | | |
| Integrity MD5 | MD5 hash value of the file computed while collecting that file (displayed in hexadecimal base16) | | Y | Y via Hash |

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

| | | | | |
|---|---|---|---|---|
| | | | | Deduplication (combines MD5/SHA1/Size) |
| Integrity SHA1 | SHA1 hash value of the original file computed while collecting that file (displayed in hexadecimal base16) | | Y | |
| Photo Probability | Probability that a picture is a photo (0: very unlikely, 70 fairly likely, 100 extremely likely) | | Y | Y |
| Visual Class | Visual classes this picture is likely to belong to | Y | Y | Y |
| Entities | Entities found in this document or text | | | Y |
| EXIF Make | Camera make found in the EXIF data of this photo | | Y | Y |
| EXIF Model | Camera model found in the EXIF data of this photo | | Y | Y |
| EXIF Camera Serial Number | Camera serial number found in the EXIT data of this photo | | Y | Y |
| EXIF Date Time | Date and time found in the EXIT data of this photo | | Y | Y |
| EXIF Coordinates | Coordinates found in the EXIT data of this photo | | Y | Y |
| Geolocation | Coordinates from the Geolocation object of the record | Y | N | Y |
| Metadata | Metadata found in this file | | | |
| Whitelist | Name of whitelist containing that file (shown only in the Files view) | | | Y |
| Collected File Path | Path of the copy of the file that was collected. This relative path starts in the scan result folder and points to the archive where the file was saved. Example: "original_files/originals_3.zip" | | Y | Y |
| Auto-Tagged | Set to true if that file was automatically tagged | Y | Y | Y |
| Captures | Capture names that processed and matched that file | | | Y |

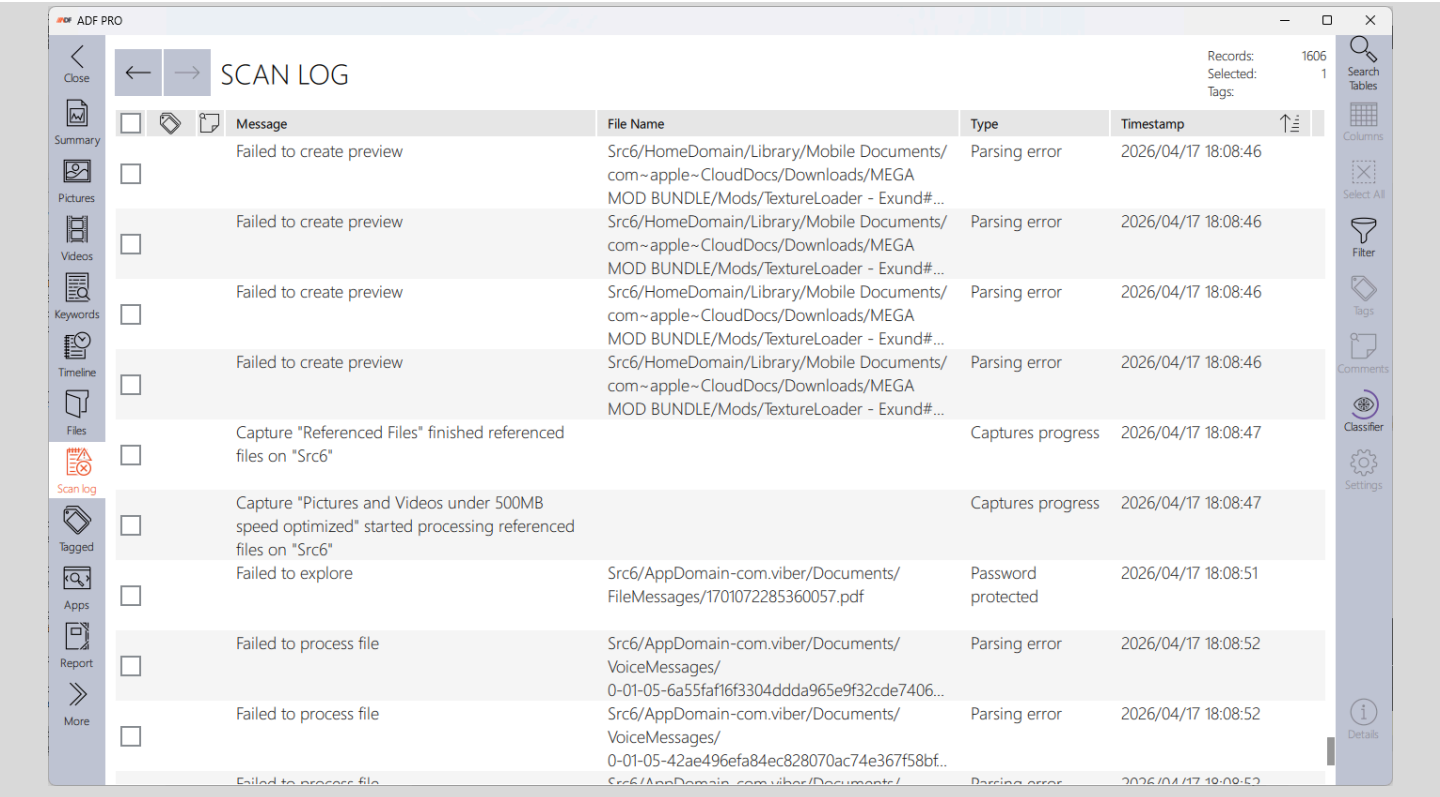
# Scan Log View

The Scan Log view shows processing events that took place during the scan. The following events are logged:

- Drive input/output errors
- Error parsing files
- Limit reached (for example 50 keywords hits in the same file)
- Password protected file encountered
- Scan progress information

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

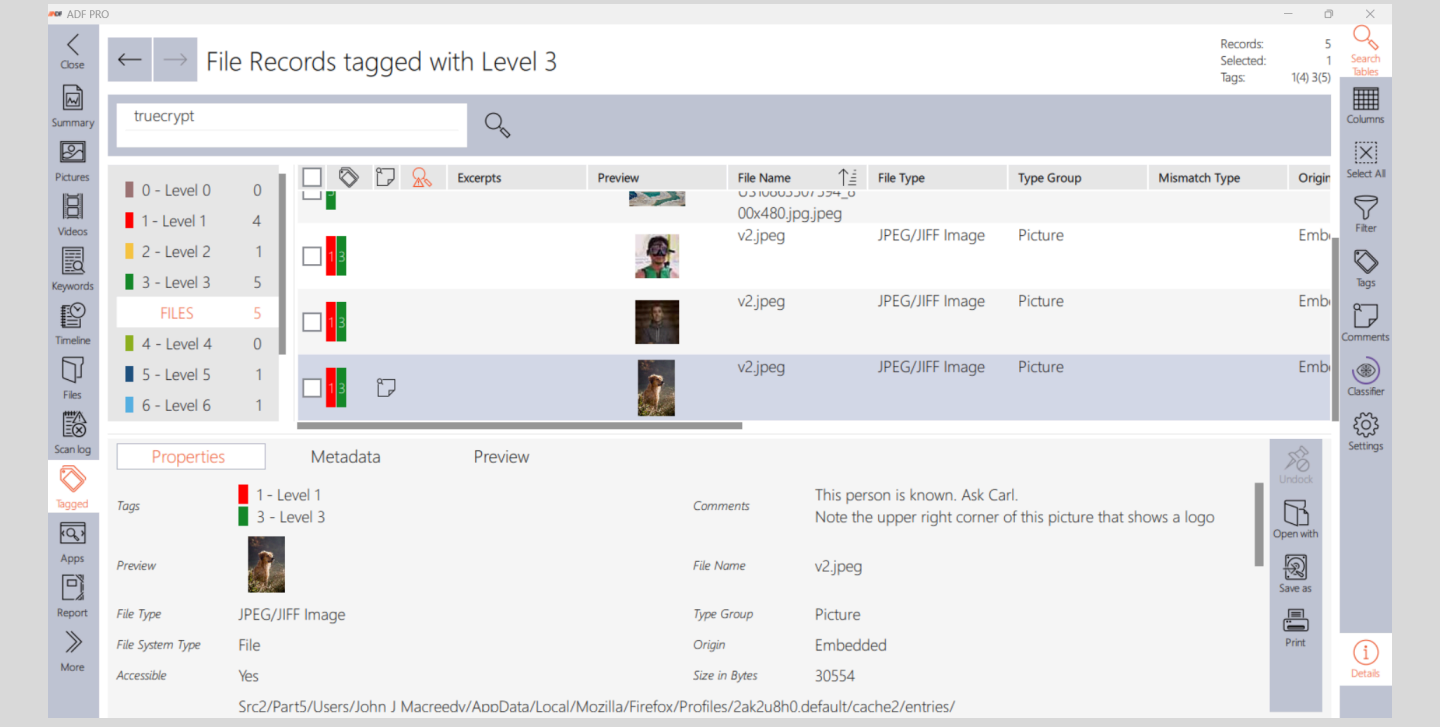
- Errors from the remote agent




# Tagged View

The Tagged view lists all the tagged records. The records are organized by tag and view and are accessible from the left-hand side list.

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.



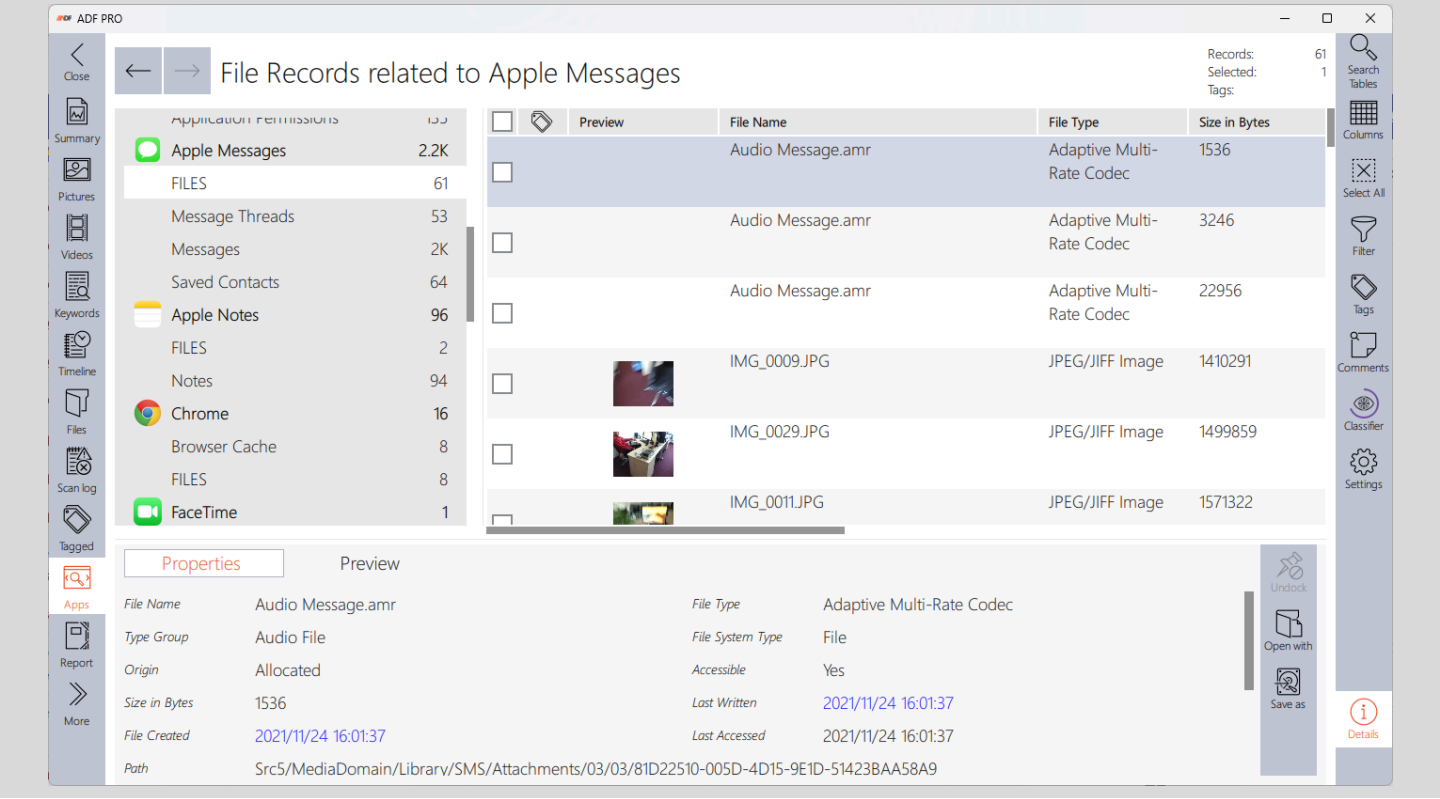

# Applications View

The Applications view lists all discovered applications. Each application is displayed with the number of related artifacts.

When an application is listed, its artifacts are grouped by type and displayed using their native tables.

- Application names are sorted alphabetically.
- Sub-groups (artifact types) are also sorted alphabetically.
- Filters, tagging, comments, export, and preview panels work as in native views.
- The **Source** column is hidden in the Applications view.
- Filters are not persisted when switching between artifact types.
- Statistics in the upper-right corner show how many records are currently filtered.

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.




# Capture Views

The Capture views show the records collected by each Capture.

## Visual Similarity (PhotoDNA) Capture View

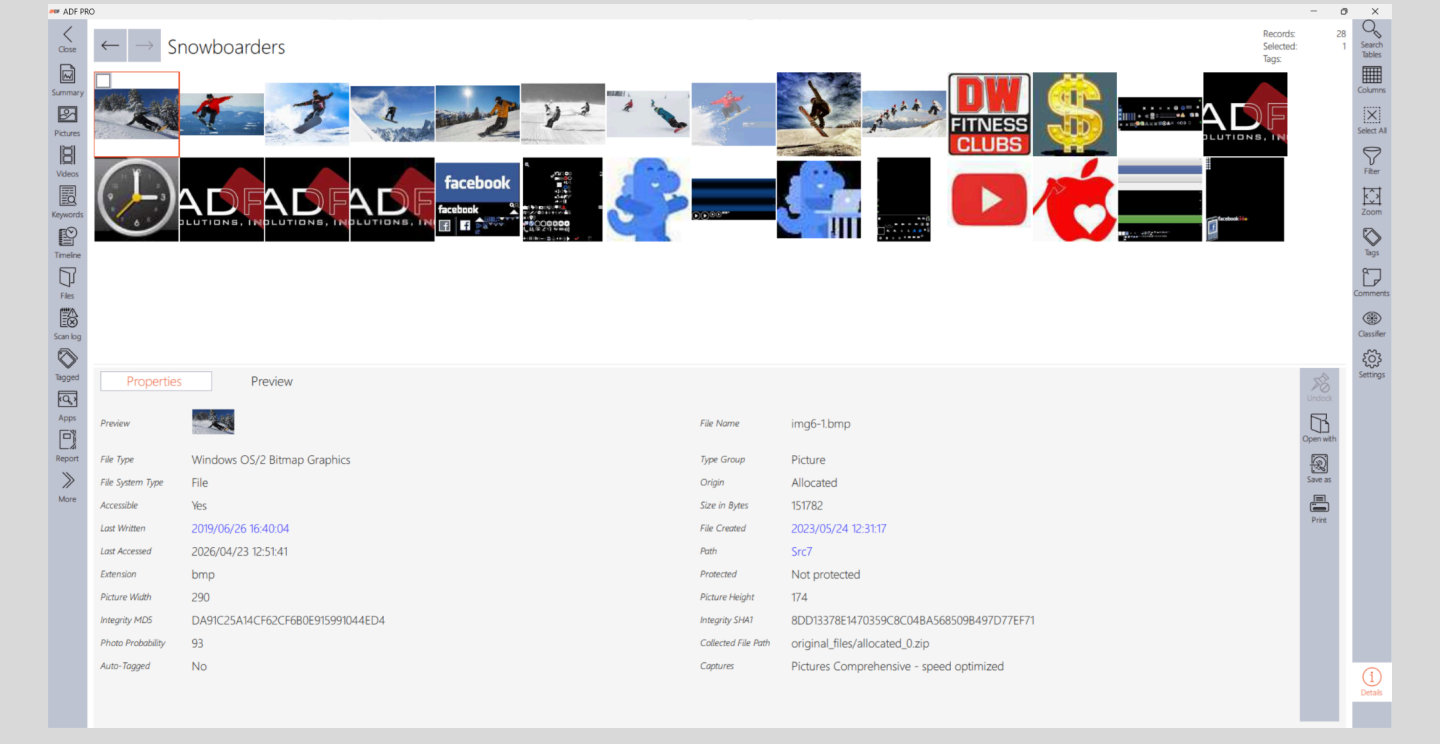
When reviewing the results of this Capture, the pictures displayed are sorted by the PhotoDNA score. Pictures that have the highest PhotoDNA score are presented first.

In this example, this picture was added to a Visual Similarity Capture.



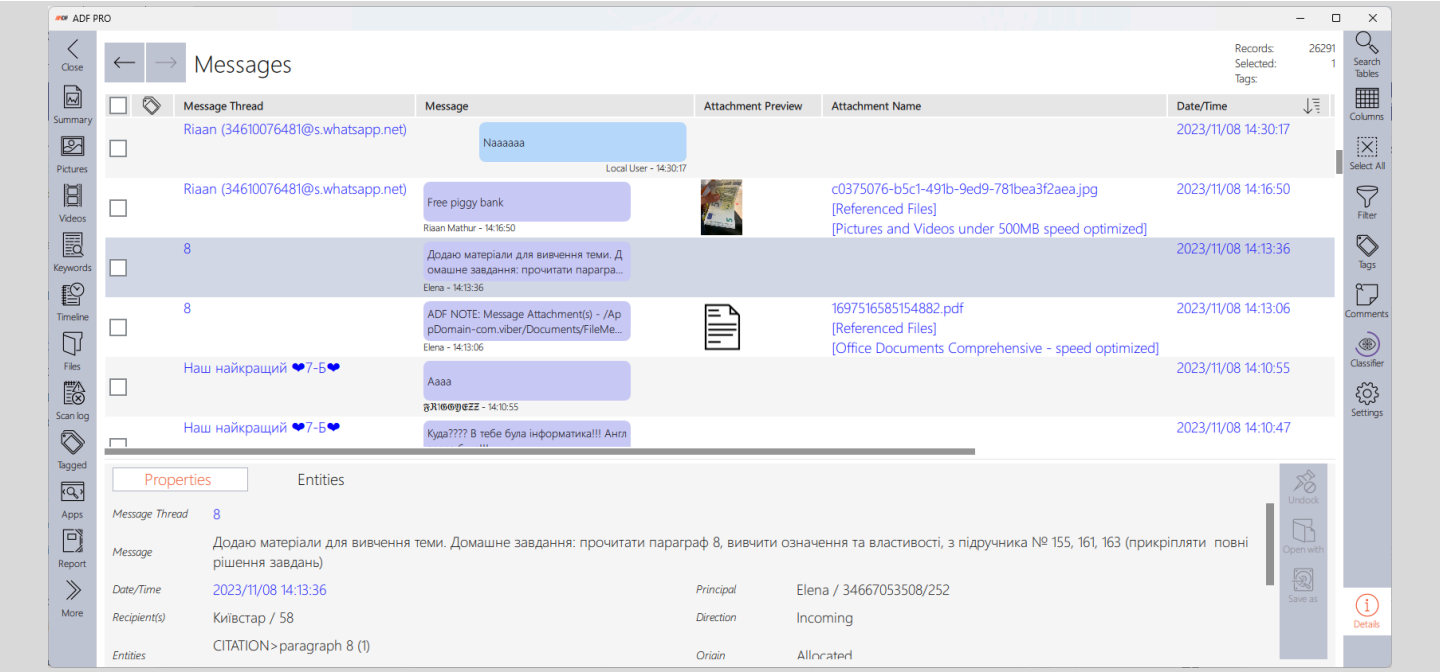
When looking at the results, the exact picture is listed first followed by the edited pictures and those from slightly different angles. Pictures containing similar buildings scored highly followed by pictures which scored lower on visual similarity.

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.




## Messages View

The Messages artifact Captures displays messages collected in Chat applications.




Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

The Messages view will display the message content in the Message column. Messages sent by the local user, known as Outgoing messages, will be displayed in a blue message bubble that is right aligned in the Message column. Messages sent from others to the local user, known as Incoming messages, will be displayed in a green message bubble and left aligned in the Message column.

The Message Thread column indicates if messages are part of a single conversation, clicking on a hyperlink in this column will filter the view to only show messages from that conversation.



If a message started with "ADF NOTE" it means that the content was edited by the ADF application to provide more context.

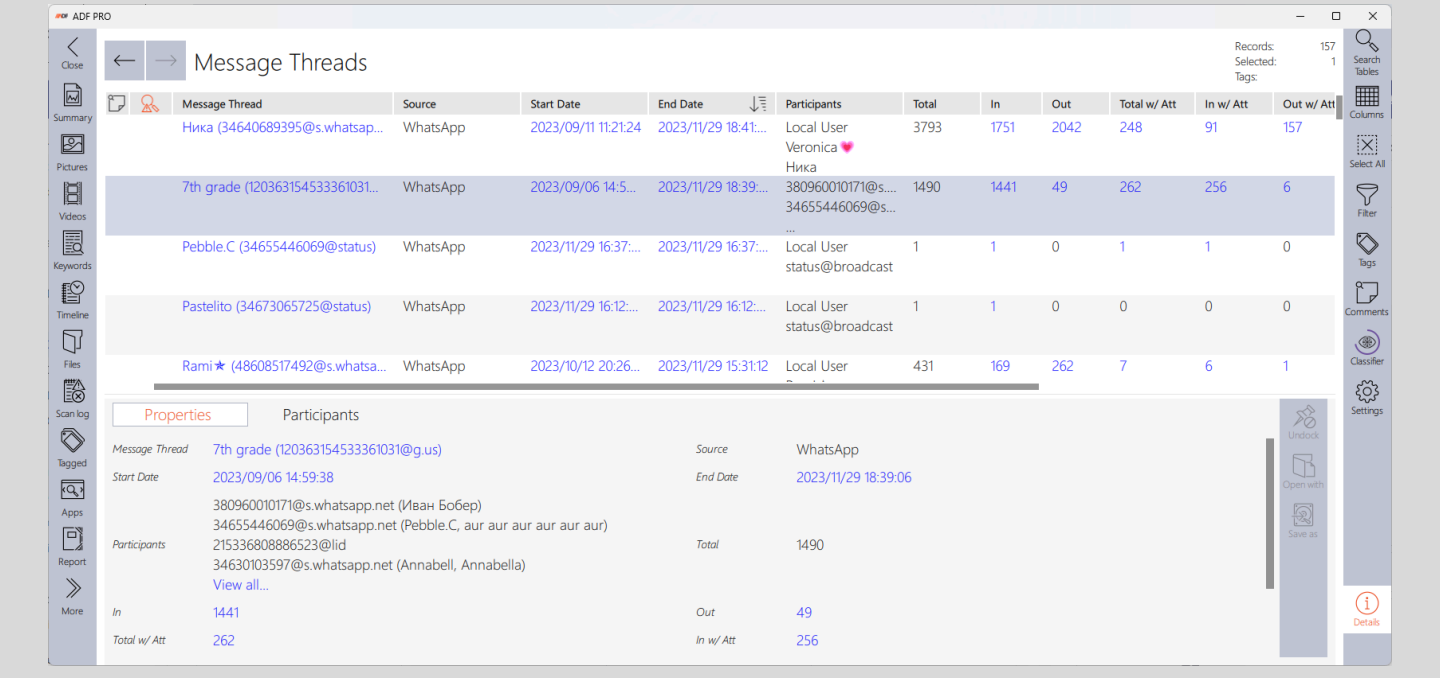
## Message Threads View

The Message Threads view displays conversations identified across all supported messaging platforms. Each record in this view represents a single message thread.

The view provides an overview of messaging activity, showing the number of messages exchanged, the participants involved, and whether attachments were shared.

When selecting a message thread, users can open the related messages directly in the Messages view by clicking on the Message Thread hyperlink. The Messages view will then be automatically filtered to show only messages from the selected conversation.

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.




## Table columns

| Field | Description |
|---|---|
| Message Thread | Unique identifier for each message thread. Displayed as a clickable hyperlink that opens the Messages view filtered by this thread ID. |
| Source | Name of the messaging platform. |
| Start Date | Timestamp of the first message in the thread. Displayed as a hyperlink to the Timeline view, showing activities that occurred around that time. |
| End Date | Timestamp of the last message in the thread. Displayed as a hyperlink to the Timeline view, showing activities that occurred around that time. |
| Participants | Displays up to two participant names or identifiers. If more participants exist, they appear as Name 1, Name 2 +x more. Hovering over the cell displays a tooltip listing all participants. When names are unavailable, phone numbers or handles are displayed. |
| Total | Total number of messages contained in the thread. Displayed as a hyperlink to the Messages view, filtered to show all messages from the selected thread. |
| In | Number of messages received by the local user in the thread. Displayed as a hyperlink to the Messages view, filtered to show only incoming messages. |

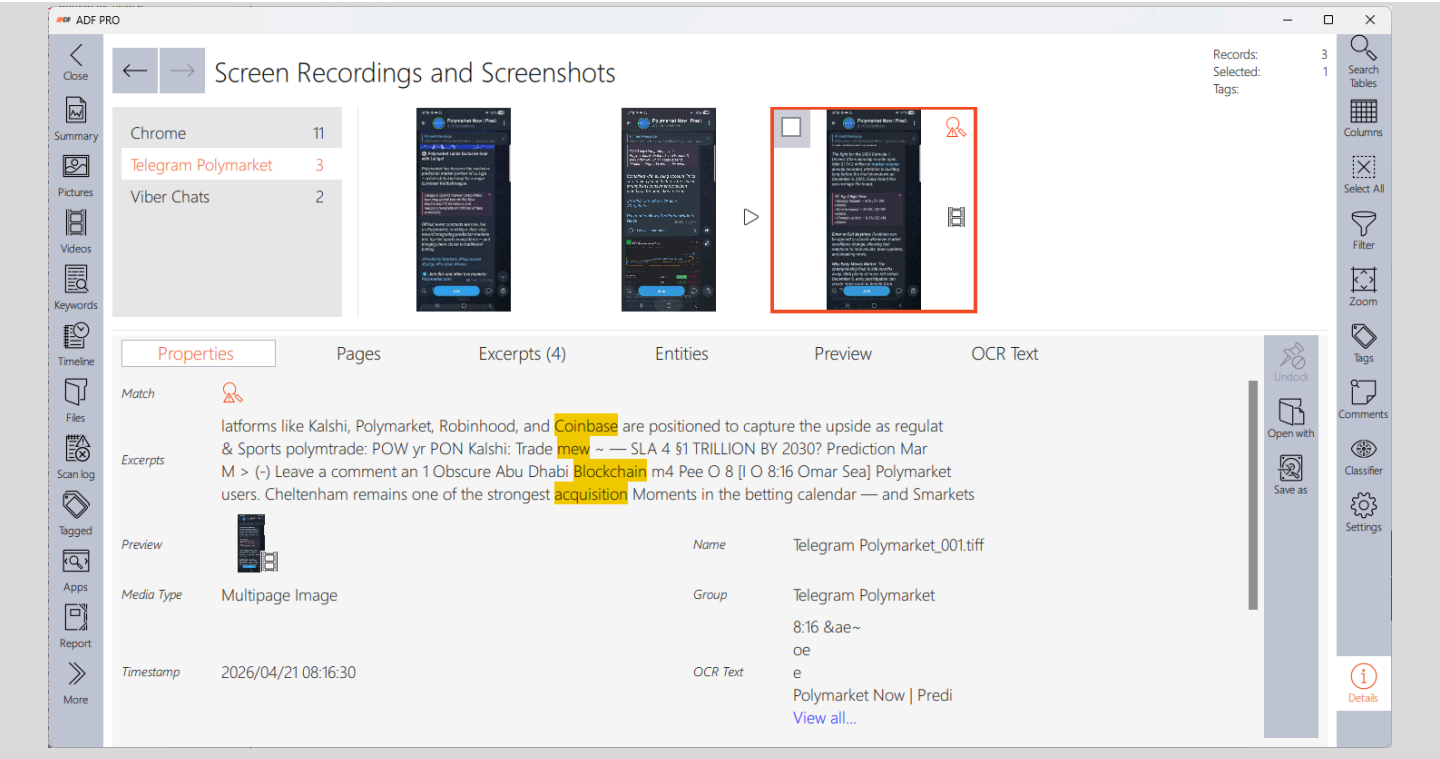
Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

| | |
|---|---|
| Out | Number of messages sent by the local user in the thread. Displayed as a hyperlink to the Messages view, filtered to show only outgoing messages. |
| Total w/ Att | Number of messages that include attachments in the thread. Displayed as a hyperlink to the Messages view, filtered to show messages containing attachments. |
| In w/ Att | Number of incoming messages containing attachments in the thread. Displayed as a hyperlink to the Messages view, filtered to show incoming messages with attachments. |
| Out w/ Att | Number of outgoing messages containing attachments in the thread. Displayed as a hyperlink to the Messages view, filtered to show outgoing messages with attachments. |

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

## Screen Recordings and Screenshots View

When screenshots/screen recordings are part of the logical acquisition, the **Screen Recordings and Screenshots** view shows their thumbnails in a gallery organized in groups.




The following properties are available for each record:

- **Comments**: comments written while taking the screenshot or video recording.
- **Name**: the screenshot name.
- **Group**: the screenshot group.
- **Timestamp**: time at which the screenshot was taken.
- **Integrity MD5**: the MD5 hash value of the screenshot that can be used to verify the integrity of the screenshot over time.
- **Textual Content**: the text extracted by the Optical Character Recognition process. The textual content is not always recognized accurately, and a visual verification should always be performed. It is possible to use the Search Tables function to search for any text that has been extracted from screenshots. Keyword search Captures can also search extracted text within screenshots if **Artifact records from other Captures** is selected within the keyword search Capture's **Search Scope** (see the Search for Keywords section of the Setting Up Scans guide for details).
  By default only English words are processed but it is possible to add other languages by following the instructions in the Optical Character Recognition of Screenshots section of the Taking Screenshots of a Mobile Device guide.
- **Entities**: entities extracted from the textual content if the Entity Extraction add-on is available.
- **Origin**: always set to Allocated.

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

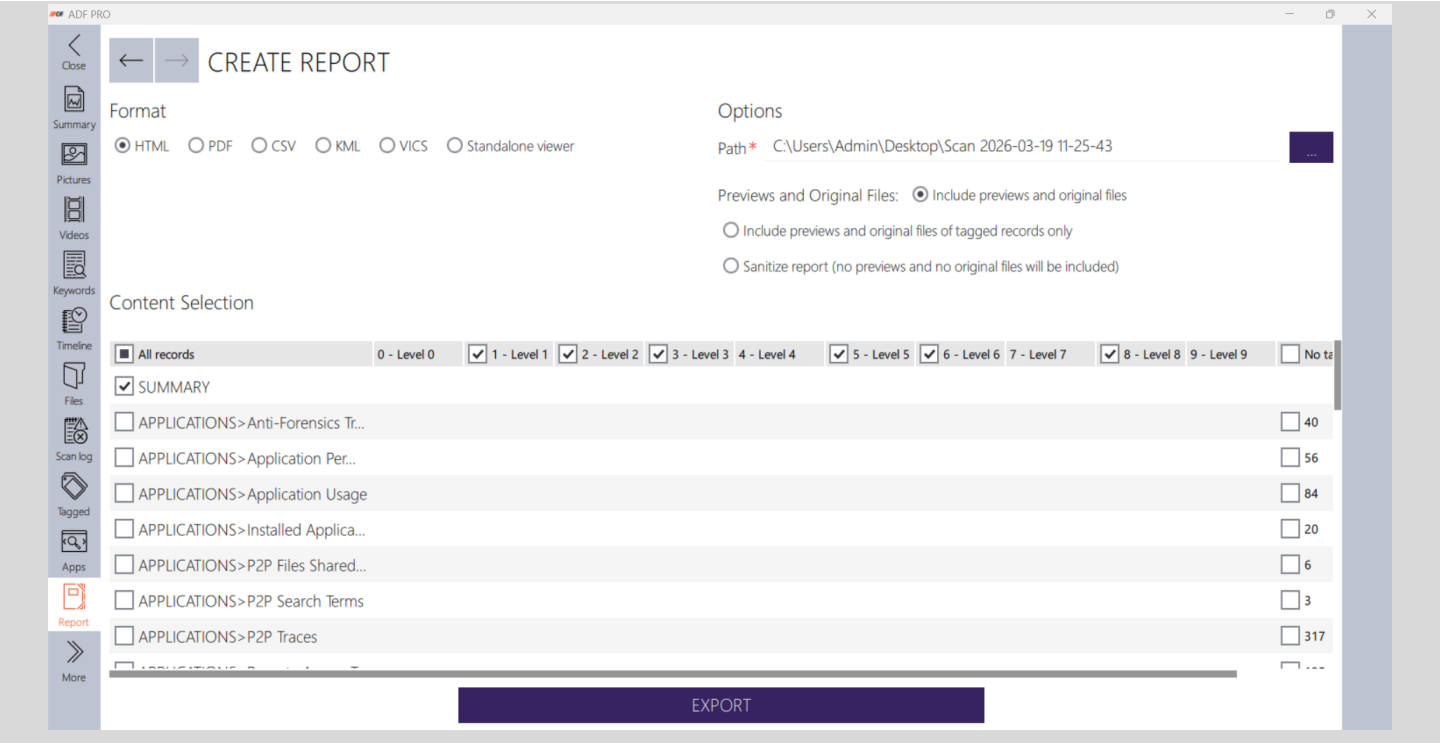
Note that the tabs of the Details panel are adjusted based on the selected item type.

# Create Report

The Report view allows the creation of reports in various formats (HTML, PDF and CSV), the creation of a Project VIC JSON file (and an export of the associated files) or the creation of a Standalone Viewer report. The Report view can be accessed from the Navigation toolbar.
Reports cannot be created when running from the Collection Key to avoid saving data on the target computer inadvertently ( DEI Digital Evidence Investigator ADFPRO Mobile & Computer Triage ).

The Create Report screen is composed of the following:

- Format: to select the report format.
- Options:
    - To choose the desired destination folder and the PDF report orientation.
    - To decide if original files and previews should be included in the report:
        - Include previews and original files: does not sanitize the report and includes original files and previews.
        - Include previews and original files of tagged records only.
        - Sanitize report (no previews and no original files will be included).
- Content Selection: to select which views and records should be part of the report.
- EXPORT button: to generate the report.




Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

## Content Selection

The Content Selection table has the following columns:

- Column 1: shows all the views that can be exported in the report.
- Column 2 to 11 (tag name): each column shows the number of records that have been tagged. These records are selected by default.
- Column 12 (No tag): shows the number of records that have not been tagged.
- Column 13 (Include original files): offers the option to include the original files associated with the selected records. Original files are exported in folders or archives and their original paths are maintained.
- Column 14 (List layout): offers the option to display each record as a vertical list of properties instead of in a table row. HTML and PDF formats only.

It is possible to select an entire column by checking the checkbox in the column header, and it is possible to select an entire row by checking the checkbox at the beginning of the row. All the records and views can be selected at once by checking the All records checkbox.



To view the description of a capture, hover your mouse over its name.



Exporting too many records may render the report impossible to open.

## HTML Report

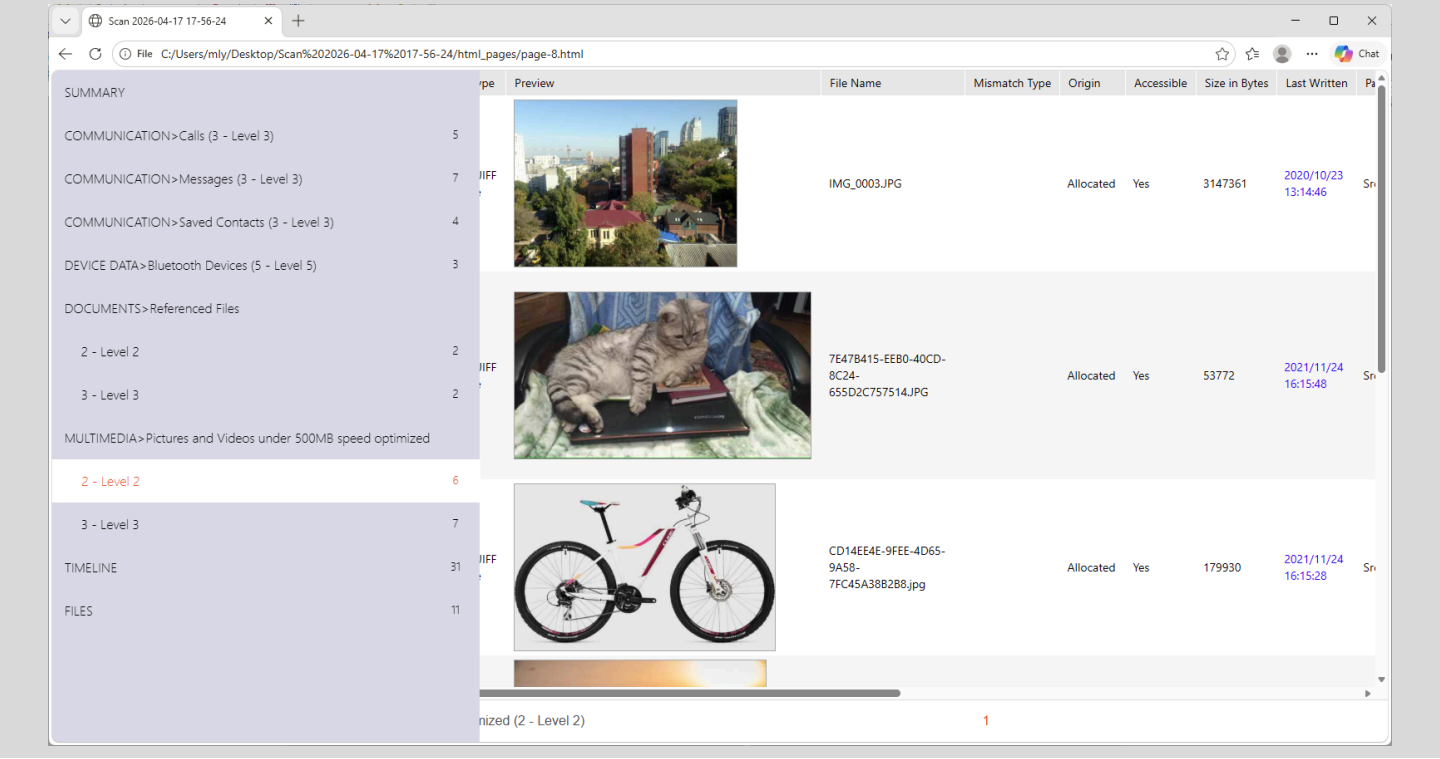
To create an HTML report that can be opened by a web browser, select the HTML format, select the destination folder, select the content, and click on the EXPORT button.

Upon creation, the following files are generated:

- REPORT_NAME - folder containing all the report files
    - html_pages - folder containing the individual pages of the report
    - original_files - folder containing the original files
    - previews - folder containing the picture previews
    - index.html - the main report file

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

The HTML report has a navigation panel on the left-hand side which expands on mouse-over and presents the exported records organized by views and by tag.




## PDF Report

To create a PDF report that can be opened by Acrobat Reader or another PDF viewer, select the PDF format, select the destination folder, select the orientation (landscape or portrait), select the content, and click on the EXPORT button.

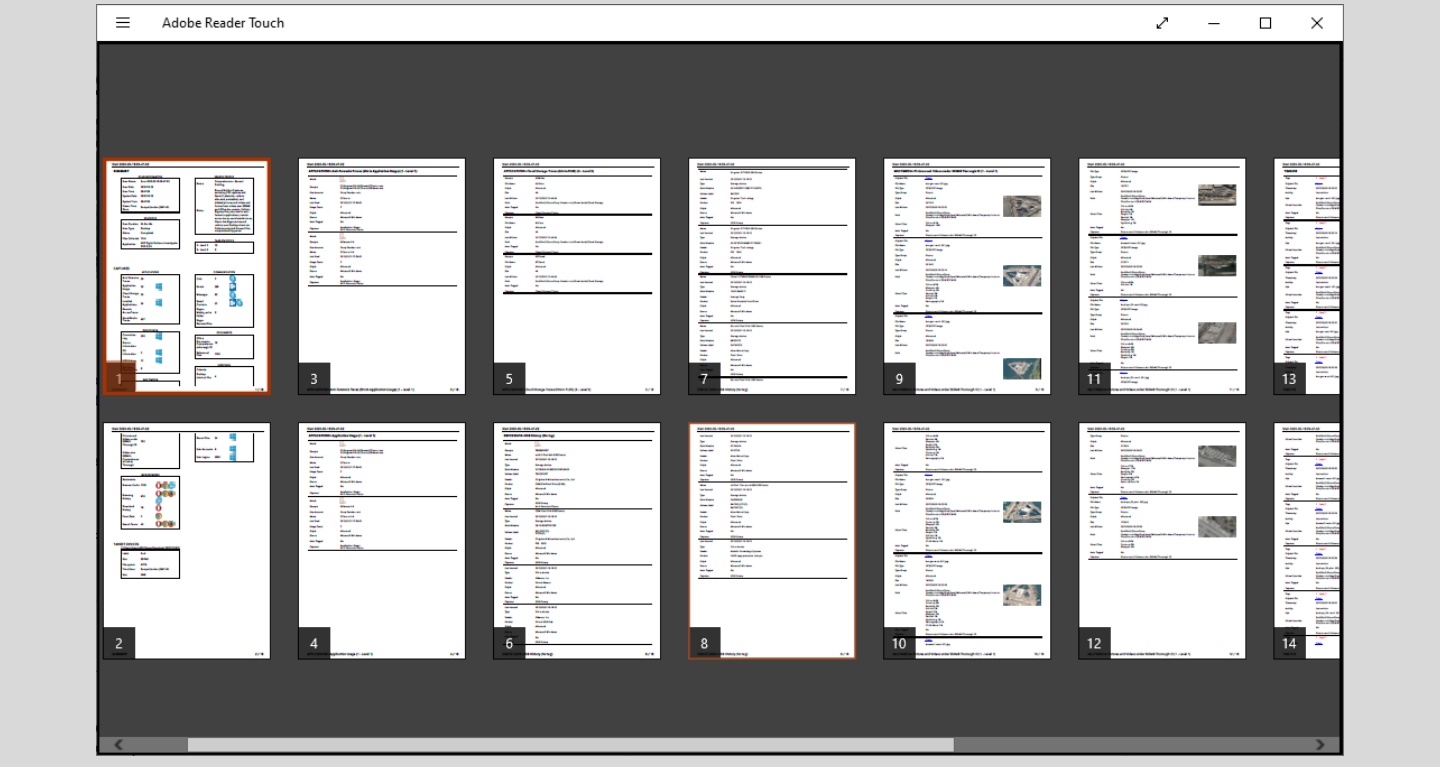
Note that by default, the List layout (column 14) is selected for all the views because it usually fits better on a PDF document than a table with many columns.
When selecting the table display instead, it is possible to limit the number of columns by hiding them in the viewer.

Upon creation, the following files are generated:

- REPORT_NAME - folder containing all the report files
  - original_files - folder containing the original files
  - scan_name.pdf - the main report file

The PDF report displays all the selected views sequentially in the order of the Content Selection table.

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.




## CSV Report

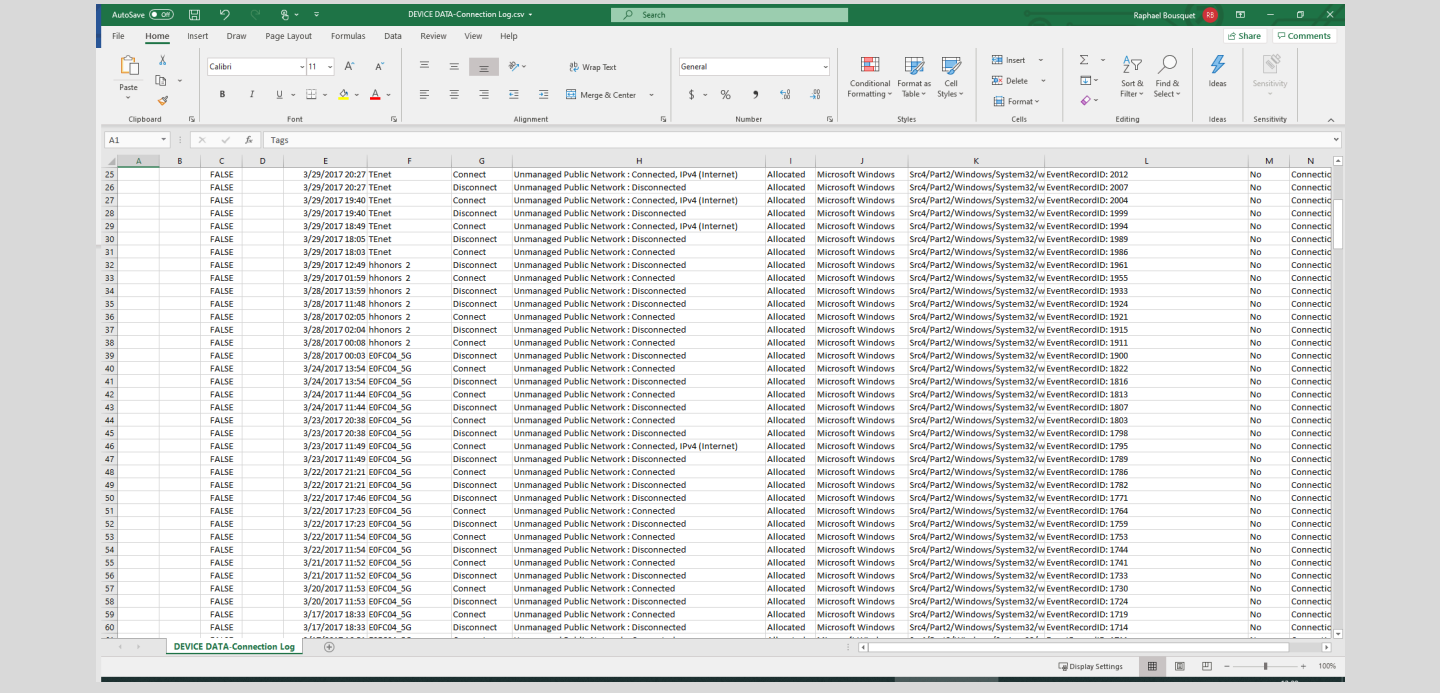
To create a CSV report that can be opened by a text editor or a spreadsheet application, select the CSV format, select the destination folder, select the content, and click on the EXPORT button. The CSV report can only contain text but the original files can still be exported.

Upon creation, the following files are generated:

- REPORT_NAME - folder containing all the report files
  - original_files - folder containing the original files
    - allocated_X.zip - archive containing matches from allocated files
    - embedded_X.zip - archive containing matches from containers
    - deleted_X.zip - archive containing matches from deleted files
    - carved_X.zip - archive containing matches from unallocated space or carved from files
  - Capture_group-Capture_name-record_type.csv - each Capture or view has its own CSV file

The record properties are all exported in the CSV files, they are not influenced by the visible columns in the viewer.

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.




## KML Report

The KML (Keyhole Markup Language) report is designed to display geospatial data using tools such as Google Earth or any KML-compatible viewer. This report provides a map-based visualization of records with geolocation information, enabling the analysis of spatial distributions.

To create a KML report, select the KML format, select the destination folder, select the content, and click on the EXPORT button.

Each record in the KML report includes:

- Image Previews - where applicable, a visual preview of the associated file is included.
- EXIF Metadata - if available.
- File Name - the original name of the file.
- File Path - the file's location within the source system.
- Source of the artifact when applicable.

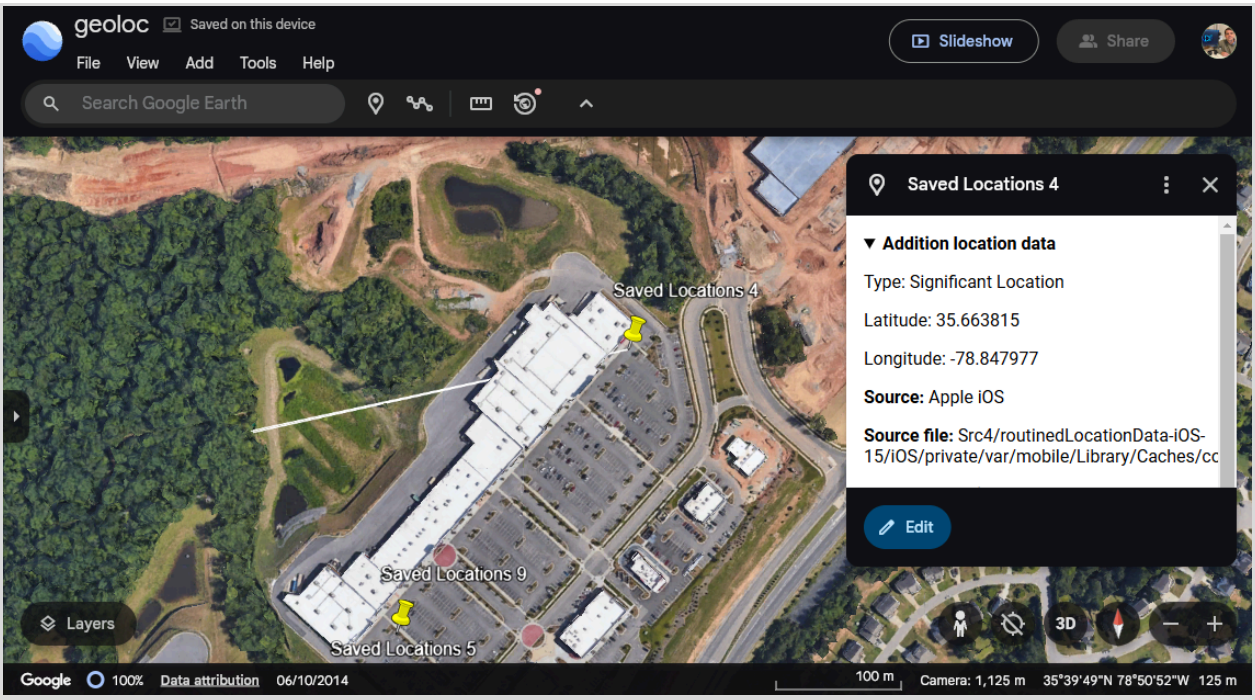
Upon creation the following files are created:

- REPORT_NAME - folder containing KML report file
    - REPORT_NAME.kml - file that can be opened with applications like Google Earth or any KML-compatible viewer.

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

Only records containing geolocation data can be included in the report.

Here is an example of how Google Earth online presents the KML report.




## VICS Report

To create a VICS report that can be opened by an application supporting the VICS data format (used by Project VIC, CAID and more), select the VICS format, select the destination folder, select the content, and click on the EXPORT button.

Upon creation, the following files are generated:

- REPORT_NAME - folder containing all the report files
  - original_files - folder containing the original files
  - scan_name.json - the main report file

Only file records with an original file can be exported.

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

## Standalone Viewer Report

To create a Standalone viewer report that contains its own executable, select the Standalone viewer format, select the content, select the destination folder, and click on the EXPORT button.

# How to use the Standalone Viewer

The Standalone viewer is a Windows executable that doesn't have to be installed and can be created when exporting a scan result as described here.



The Standalone Viewer can be used without a license, so it can be distributed easily.

When creating a Standalone viewer from the Report screen, the following folders are created:

- *SCAN_NAME*
  - *ScanResults* - folder containing the scan result
  - *win* - folder containing the Standalone viewer executable
  - ADF Viewer.bat - file to start the Standalone viewer

When starting the Standalone viewer, the first screen shows the scan results present in the local ScanResults folder and offers the following actions for each scan result:

| | |
|---|---|
|  Report | To open the scan result on the report creation screen. |
|  View | To view the scan result. Double-clicking on the scan result also selects this action. |

The right-hand side function toolbar offers the following actions:

| | |
|---|---|
|  Quit | To close the application immediately. |

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

| | |
|---|---|
|  Open | To open a scan result not located in the local ScanResults folder. |
|  Guide | To open this guide. |
|  About | Open the 'About Standalone Viewer' dialog to see the product and version. |

The Standalone viewer offers the same function as the application viewer except for the following:

- It is not possible to delete a scan result.
- The post-scan tasks (image classification, video classification, etc) are not executed.



The Standalone viewer has to be executed from a medium with read and write access as it needs to save logs and user actions.

Copyright ©2016-2025 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.