Reviewing Scan Results

Introduction

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

This document applies to the following applications		
ADF PRO PRO	Digital Evidence Investigator DEI	Mobile Device Investigator MDI

What are Scan Results?

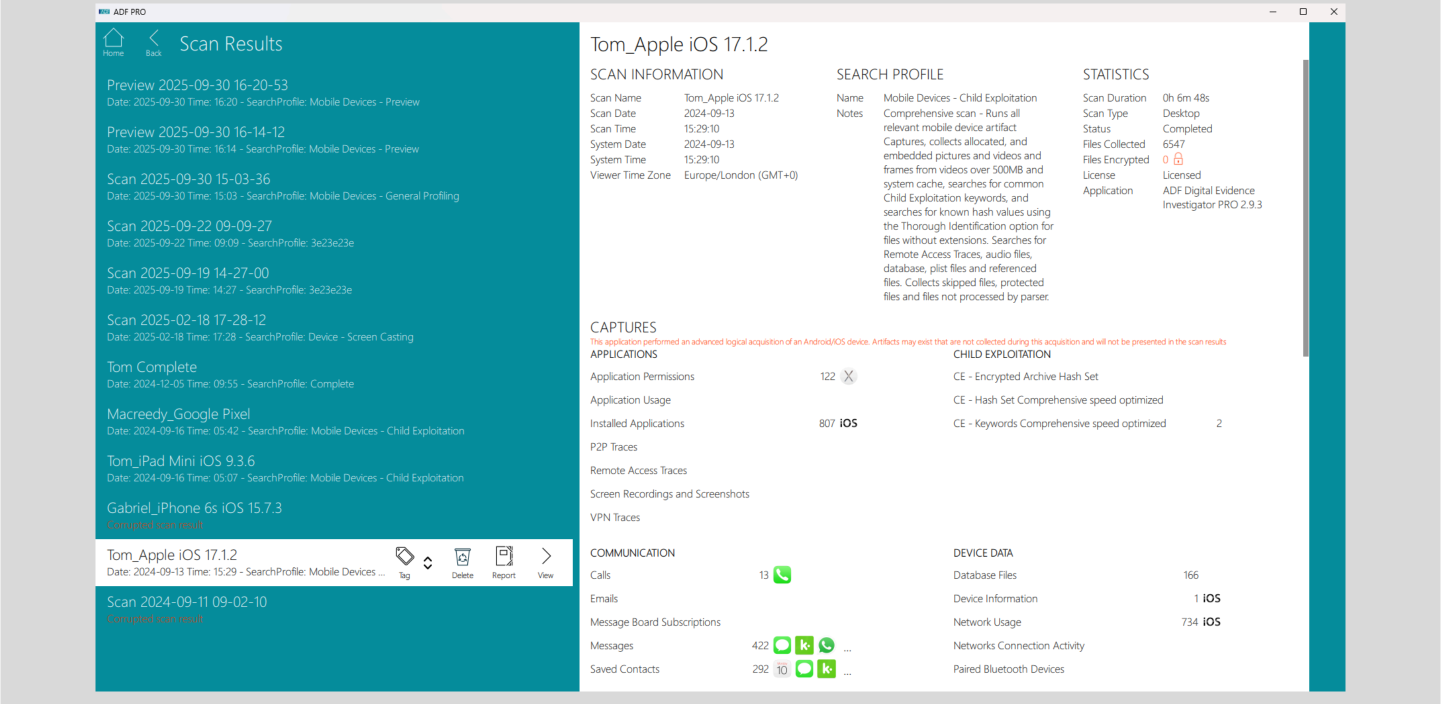
Scan results are created during the scan of a target device or logical data. They contain records of files and artifacts identified by the Captures for matching precise search criteria.
Scan results can be reviewed by navigating through records, filtering, sorting, tagging, commenting, and creating a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

Select Scan Result



Scan Results

Preview 2025-09-30 16-20-53
Date: 2025-09-30 Time: 16:20 - SearchProfile: Mobile Devices - Preview

Preview 2025-09-30 16-14-12
Date: 2025-09-30 Time: 16:14 - SearchProfile: Mobile Devices - Preview

Scan 2025-09-30 15-03-36
Date: 2025-09-30 Time: 15:03 - SearchProfile: Mobile Devices - General Profiling

Scan 2025-09-22 09-09-27
Date: 2025-09-22 Time: 09:09 - SearchProfile: 3e23e23e

Scan 2025-09-19 14-27-00
Date: 2025-09-19 Time: 14:27 - SearchProfile: 3e23e23e

Scan 2025-02-18 17-28-12
Date: 2025-02-18 Time: 17:28 - SearchProfile: Device - Screen Casting

Tom Complete
Date: 2024-12-05 Time: 09:55 - SearchProfile: Complete

Macreedy_Google Pixel
Date: 2024-09-16 Time: 05:42 - SearchProfile: Mobile Devices - Child Exploitation

Tom_iPad Mini iOS 9.3.6
Date: 2024-09-16 Time: 05:07 - SearchProfile: Mobile Devices - Child Exploitation

Gabriel_iPhone 6s iOS 15.7.3
Corrupted scan result

Tom_Apple iOS 17.1.2
Date: 2024-09-13 Time: 15:29 - SearchProfile: Mobile Devices ...

Scan 2024-09-11 09-02-10
Corrupted scan result

Tom_Apple iOS 17.1.2

SCAN INFORMATION

Scan Name	Tom_Apple iOS 17.1.2
Scan Date	2024-09-13
Scan Time	15:29:10
System Date	2024-09-13
System Time	15:29:10
Viewer Time Zone	Europe/London (GMT+0)

SEARCH PROFILE

Name	Mobile Devices - Child Exploitation
Notes	Comprehensive scan - Runs all relevant mobile device artifact Captures, collects allocated, and embedded pictures and videos and frames from videos over 500MB and system cache, searches for common Child Exploitation keywords, and searches for known hash values using the Thorough Identification option for files without extensions. Searches for Remote Access Traces, audio files, database, plist files and referenced files. Collects skipped files, protected files and files not processed by parser.

STATISTICS

Scan Duration	0h 6m 48s
Scan Type	Desktop
Status	Completed
Files Collected	6547
Files Encrypted	0
License	Licensed
Application	ADF Digital Evidence Investigator PRO 2.9.3

CAPTURES

This application performed an advanced logical acquisition of an Android/iOS device. Artifacts may exist that are not collected during this acquisition and will not be presented in the scan results

APPLICATIONS		CHILD EXPLOITATION	
Application Permissions	122	CE - Encrypted Archive Hash Set	
Application Usage		CE - Hash Set Comprehensive speed optimized	
Installed Applications	807 iOS	CE - Keywords Comprehensive speed optimized	2
P2P Traces			
Remote Access Traces			
Screen Recordings and Screenshots			
VPN Traces			

COMMUNICATION		DEVICE DATA	
Calls	13	Database Files	166
Emails		Device Information	1 iOS
Message Board Subscriptions		Network Usage	734 iOS
Messages	422 ...	Networks Connection Activity	
Saved Contacts	292 ...	Paired Bluetooth Devices	

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. 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).
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.

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 (PRO DEi), 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:

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.

To view the description of an artifact capture, hover your 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:

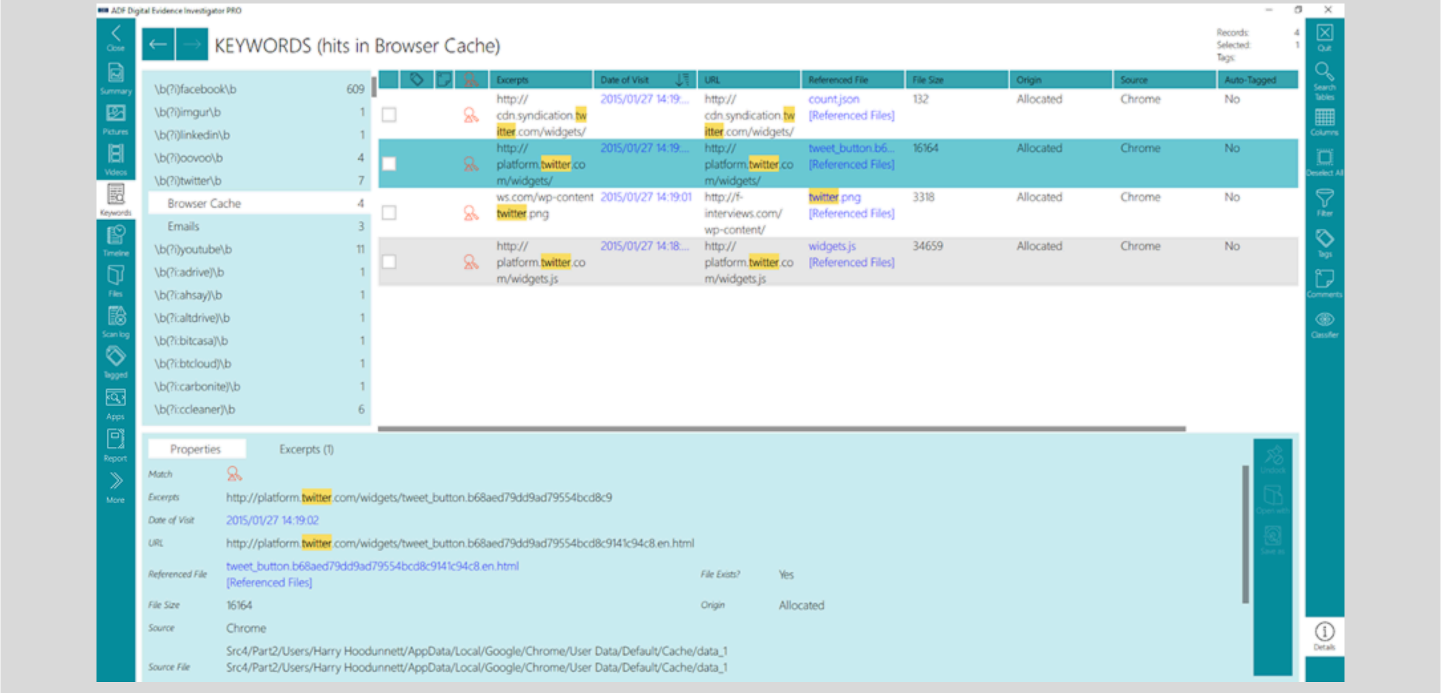
- For a drive
  - Name
  - Label (SrcN by default or defined prior to the scan)
  - Serial number
  - Bus type
  - Sector size
  - Size
  - Partition table type
    - Partition details:
    - Mount letter name
    - Size
    - File system
    - Time Zone (if the partition contains an Operating System 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 (PRO MDI)
    - Name
- For a mobile device acquisition (PRO MDI)
    - 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 (PRO MDI)
    - 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.



KEYWORDS (hits in Browser Cache)

Records: 4
Selected: 1
Tags:

\b(?i)facebook\b	609
\b(?i)imgur\b	1
\b(?i)linkedin\b	1
\b(?i)oovoo\b	4
\b(?i)twitter\b	7
Browser Cache	4
Emails	3
\b(?i)youtube\b	11
\b(?i:adrive)\b	1
\b(?i:ahsay)\b	1
\b(?i:altdrive)\b	1
\b(?i:bitcasa)\b	1
\b(?i:btcloud)\b	1
\b(?i:carbonite)\b	1
\b(?i:ccleaner)\b	6

				Excerpts	Date of Visit	URL	Referenced File	File Size	Origin	Source	Auto-Tagged
□				http://cdn.syndication.twitter.com/widgets/	2015/01/27 14:19:...	http://cdn.syndication.twitter.com/widgets/	count.json [Referenced Files]	132	Allocated	Chrome	No
□				http://platform.twitter.com/widgets/	2015/01/27 14:19:...	http://platform.twitter.com/widgets/	tweet_button.b6... [Referenced Files]	16164	Allocated	Chrome	No
□				ws.com/wp-content twitter.png	2015/01/27 14:19:01	http://f-interviews.com/wp-content/	twitter.png [Referenced Files]	3318	Allocated	Chrome	No
□				http://platform.twitter.com/widgets.js	2015/01/27 14:18:...	http://platform.twitter.com/widgets.js	widgets.js [Referenced Files]	34659	Allocated	Chrome	No

Properties Excerpts (1)

Match

Excerpts http://platform.twitter.com/widgets/tweet_button.b68aed79dd9ad79554bcd8c9

Date of Visit 2015/01/27 14:19:02

URL http://platform.twitter.com/widgets/tweet_button.b68aed79dd9ad79554bcd8c9141c94c8.en.html

Referenced File tweet_button.b68aed79dd9ad79554bcd8c9141c94c8.en.html [Referenced Files]

File Exists? Yes

File Size 16164

Origin Allocated

Source Chrome

Source File Src4/Part2/Users/Harry Hoodunnett/AppData/Local/Google/Chrome/User Data/Default/Cache/data_1
Src4/Part2/Users/Harry Hoodunnett/AppData/Local/Google/Chrome/User Data/Default/Cache/data_1

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.

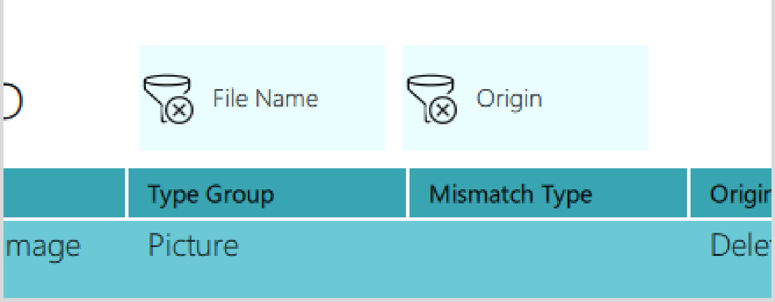
←	To move backward in the view history. Hold to see history.
→	To move forward in the view history. Hold to see history.

View Title Panel

This panel shows the name of the view being displayed.

Filter Summary Panel

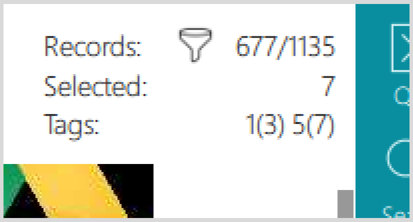
When filters are applied, the name of the filtered column is displayed in that panel. It is also possible to remove that filter by clicking on the funnel icon.



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)



Records: 677/1135
Selected: 7
Tags: 1(3) 5(7)

Navigation Toolbar

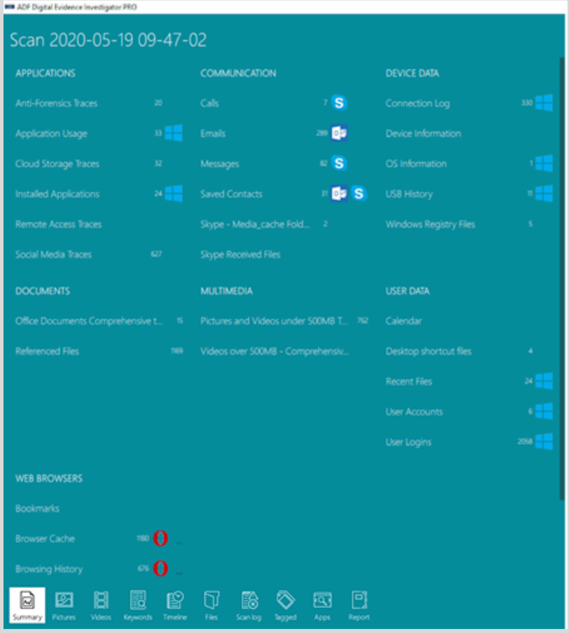
Located vertically on the left-hand side of the screen is the navigation toolbar. This toolbar will allow navigation through the results. The following buttons are located on this toolbar:

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.
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.



ADF Digital Evidence Investigator PRO

Scan 2020-05-19 09-47-02

APPLICATIONS

Anti-Forensics Traces 20
Application Usage 33
Cloud Storage Traces 32
Installed Applications 24
Remote Access Traces
Social Media Traces 627

COMMUNICATION

Calls 7
Emails 289
Messages 82
Saved Contacts 31
Skype - Media_cache Fold... 2
Skype Received Files

DEVICE DATA

Connection Log 330
Device Information
OS Information 1
USB History 11
Windows Registry Files 5

DOCUMENTS

Office Documents Comprehensive t... 15
Referenced Files 1169

MULTIMEDIA

Pictures and Videos under 500MB T... 762
Videos over 500MB - Comprehensiv...

USER DATA

Calendar
Desktop shortcut files 4
Recent Files 24
User Accounts 6
User Logins 2058

WEB BROWSERS

Bookmarks
Browser Cache 1180
Browsing History 676

Function Toolbar

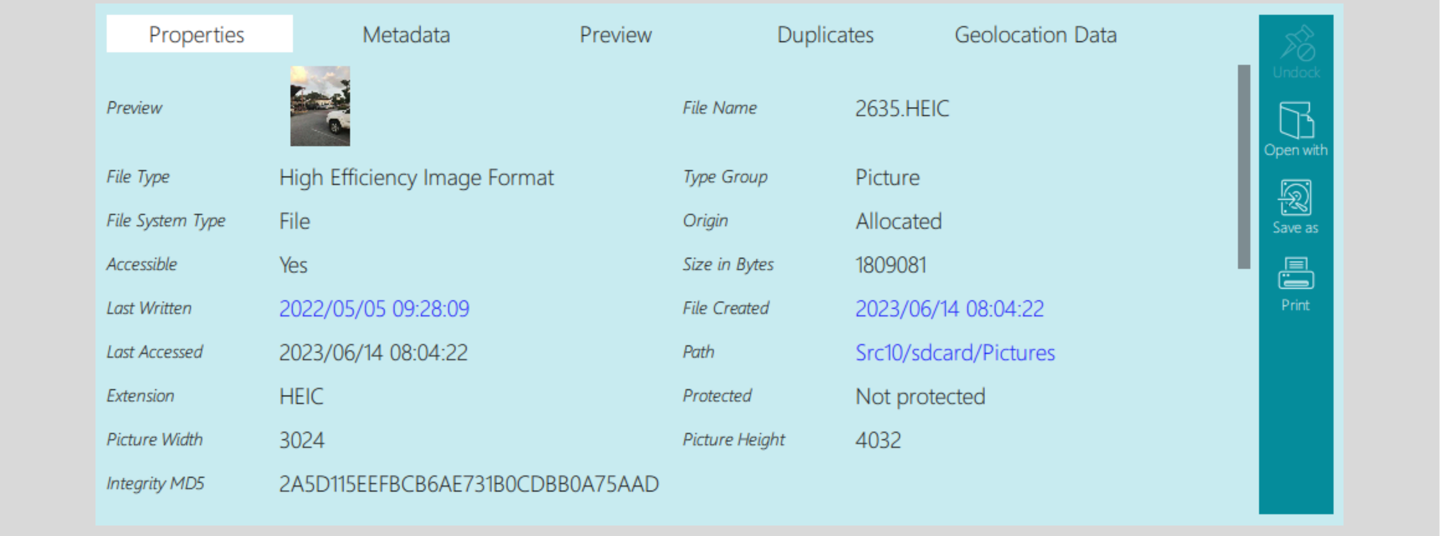
A function toolbar is located vertically on the right-hand side of the screen. This toolbar is context specific and will adapt depending on what is being viewed.

☒ 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. To adjust the sort order of displayed results. Changes made to columns display also modify columns displayed within the reports.

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). To pause and resume these post-scan tasks. 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. 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.

Details Panel

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



Preview		*File Name*	2635.HEIC
File Type	High Efficiency Image Format	*Type Group*	Picture
File System Type	File	*Origin*	Allocated
Accessible	Yes	*Size in Bytes*	1809081
Last Written	2022/05/05 09:28:09	*File Created*	2023/06/14 08:04:22
Last Accessed	2023/06/14 08:04:22	*Path*	Src10/sdcard/Pictures
Extension	HEIC	*Protected*	Not protected
Picture Width	3024	*Picture Height*	4032
Integrity MD5	2A5D115EEFBCB6AE731B0CDBB0A75AAD		

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 (PRO MDI).
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. Videos are playable via an internal player subject to locally installed codecs. Documents and other files may be viewed by clicking the Undock button on the toolbar. Multi-page screenshots are displayed alongside the extracted text.
Duplicates	Displays a list of duplicate files. Duplicate files are identified based on the hash value of their content only.

Geolocation Data	Displays geolocation data extracted from the selected record, including latitude, longitude, altitude, absolute altitude, latitude and longitude accuracy, and timestamp, if available.

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.
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)
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. Accessible in the Column panel of the functional toolbar. Accessible by clicking and dragging the column header.
Sort ascending	To sort the records in ascending order. Accessible in the Column panel of the functional toolbar. Accessible by clicking on the column header.

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

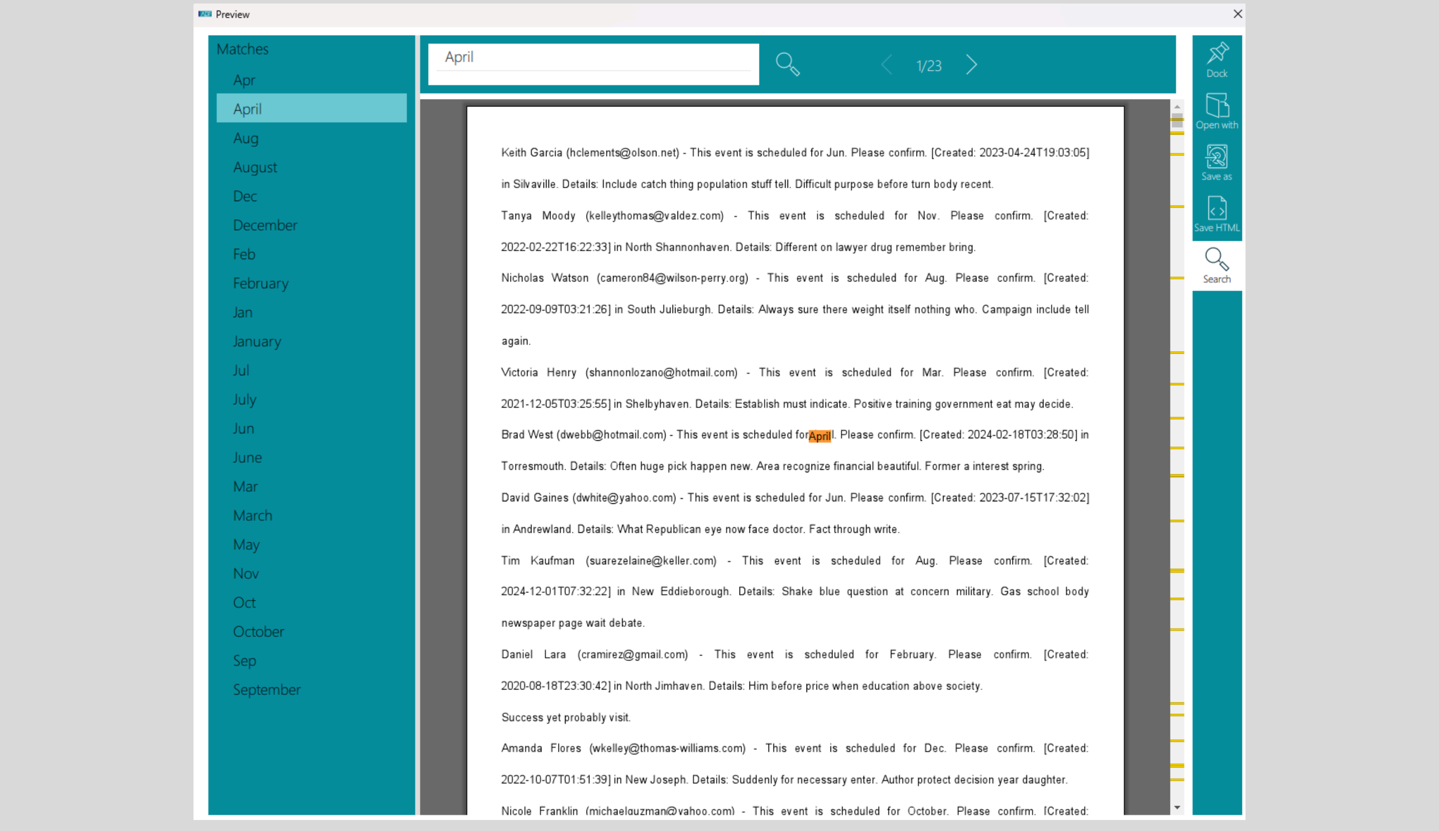
For each view, the visible columns, their position, and sort order is maintained when creating a report. Hiding columns such as the Preview column can help sanitize a report.

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.

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.



Keith Garcia (hclements@olson.net) - This event is scheduled for Jun. Please confirm. [Created: 2023-04-24T19:03:05] in Silvaville. Details: Include catch thing population stuff tell. Difficult purpose before turn body recent.

Tanya Moody (kelleythomas@valdez.com) - This event is scheduled for Nov. Please confirm. [Created: 2022-02-22T16:22:33] in North Shannonhaven. Details: Different on lawyer drug remember bring.

Nicholas Watson (cameron84@wilson-perry.org) - This event is scheduled for Aug. Please confirm. [Created: 2022-09-09T03:21:26] in South Julieburgh. Details: Always sure there weight itself nothing who. Campaign include tell again.

Victoria Henry (shannonlozano@hotmail.com) - This event is scheduled for Mar. Please confirm. [Created: 2021-12-05T03:25:55] in Shelbyhaven. Details: Establish must indicate. Positive training government eat may decide.

Brad West (dwebb@hotmail.com) - This event is scheduled forAprill. Please confirm. [Created: 2024-02-18T03:28:50] in Torresmouth. Details: Often huge pick happen new. Area recognize financial beautiful. Former a interest spring.

David Gaines (dwhite@yahoo.com) - This event is scheduled for Jun. Please confirm. [Created: 2023-07-15T17:32:02] in Andrewland. Details: What Republican eye now face doctor. Fact through write.

Tim Kaufman (suarezelaine@keller.com) - This event is scheduled for Aug. Please confirm. [Created: 2024-12-01T07:32:22] in New Eddieborough. Details: Shake blue question at concern military. Gas school body newspaper page wait debate.

Daniel Lara (cramirez@gmail.com) - This event is scheduled for February. Please confirm. [Created: 2020-08-18T23:30:42] in North Jimhaven. Details: Him before price when education above society. Success yet probably visit.

Amanda Flores (wkelley@thomas-williams.com) - This event is scheduled for Dec. Please confirm. [Created: 2022-10-07T01:51:39] in New Joseph. Details: Suddenly for necessary enter. Author protect decision year daughter.

Nicole Franklin (michaelguzman@yahoo.com) - This event is scheduled for October. Please confirm. [Created:

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
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.

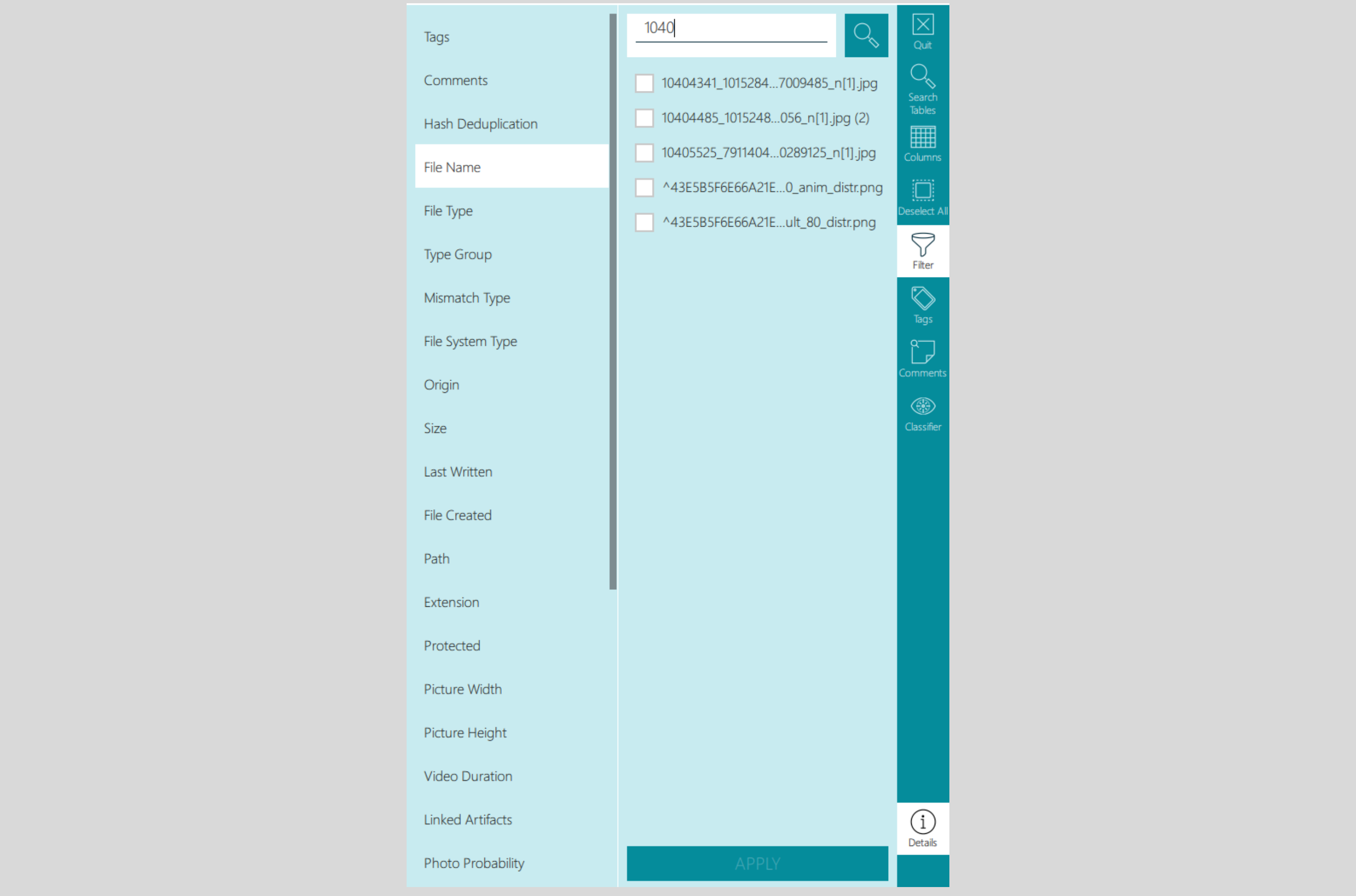
Action	Method
Select one record.	Mouse left click or touch screen tap.
Select all the records.	Keyboard Ctrl + A.
Select the record with the focus.	Keyboard Spacebar.
Select multiple records.	Select the first record then Shift+mouse left click on the last record.
Select all the fully visible records.	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.
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.



1040

□ 10404341_1015284...7009485_n[1].jpg
□ 10404485_1015248...056_n[1].jpg (2)
□ 10405525_7911404...0289125_n[1].jpg
□ ^43E5B5F6E66A21E...0_anim_distr.png
□ ^43E5B5F6E66A21E...ult_80_distr.png

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.

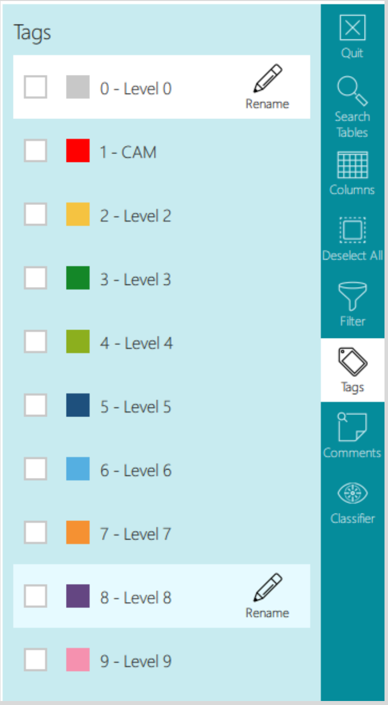
> The sort order of each view is maintained when creating a report.

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.



Tags

- □ ◼ 0 - Level 0 Rename
- □ 🟥 1 - CAM
- □ 🟨 2 - Level 2
- □ 🟩 3 - Level 3
- □ 🟩 4 - Level 4
- □ 🟦 5 - Level 5
- □ 🟦 6 - Level 6
- □ 🟧 7 - Level 7
- □ 🟪 8 - Level 8 Rename
- □ 🟥 9 - Level 9

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
Tag one or more records.	After selecting the record(s): ● Open the Tags panel and check the appropriate tag checkboxes. ● Or, press the number key 0-9 as appropriate. Note that after assigning a tag to one record, the next record is automatically selected. In a table view, tags are visible in the Tag column (🏷) and represented by a rectangle. In a gallery view, tags are represented by a rectangle at the bottom of the thumbnail (for thumbnails greater than 96 pixels). 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): ● Open the Tags panel and uncheck the appropriate tag checkboxes. ● Or, press the number key 0-9 corresponding to the tag to be removed.

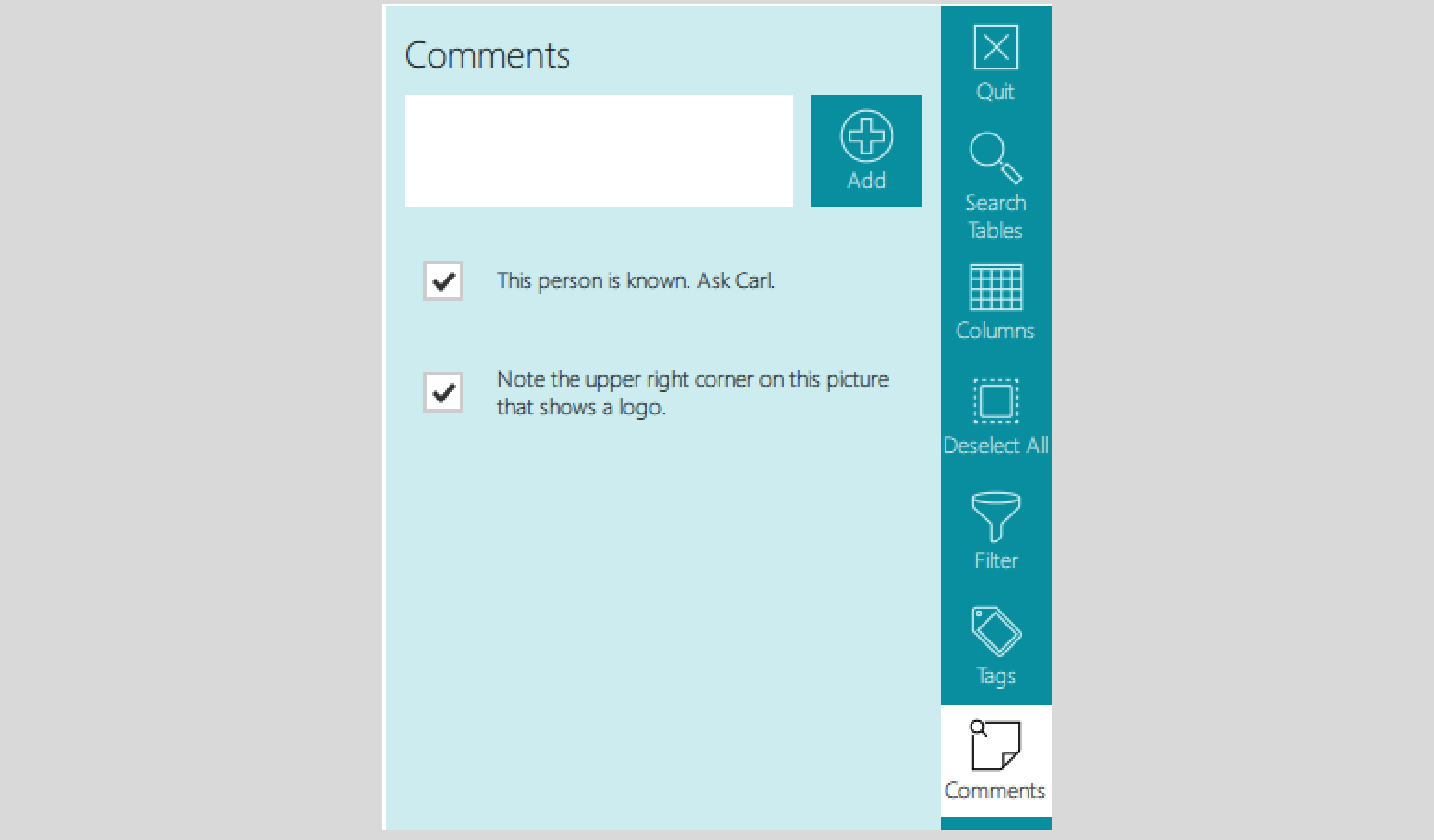
Tags are a useful way to select the content that later gets exported into a report.

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.



☑ This person is known. Ask Carl.

☑ Note the upper right corner on this picture that shows a logo.

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.

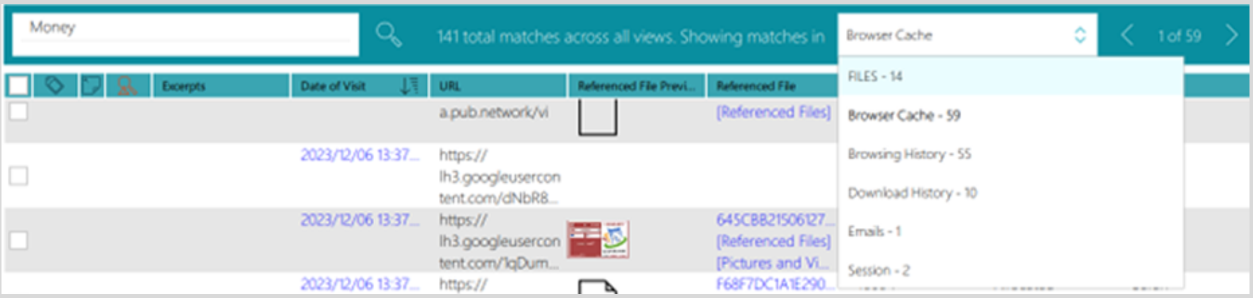
Action	Method
Assign a new comment to one or more records.	After selecting the record(s): • Open the Comments panel and type the new comment in the edit box, then click the Add button. In a table view, comments are visible in the Comment column (🗒) and represented by a similar icon. In a gallery view, 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): • 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.

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): ● 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.



Money

141 total matches across all views. Showing matches in Browser Cache

□	Excerpts	Date of Visit	URL	Referenced File Previ...	Referenced File
□			a.pub.network/vi		[Referenced Files]
□		2023/12/06 13:37...	https:// lh3.googleusercon tent.com/dNbR8...		
□		2023/12/06 13:37...	https:// lh3.googleusercon tent.com/1qDum...		645CBB21506127... [Referenced Files] [Pictures and Vi...
		2023/12/06 13:37...	https://		F68F7DC1A1E290...

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

Action	Method
Execute a keyword search	Open the Search Tables panel from the function toolbar and type the keyword in the edit box.

	The keyword entered can only be matched against the beginning of words and it is case insensitive. 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 indicates how many matches have been found and the number of the current match. Use the left (<) and right (>) arrow buttons to navigate through the results. The navigation will automatically change the view according to where the matching keyword was found. 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.

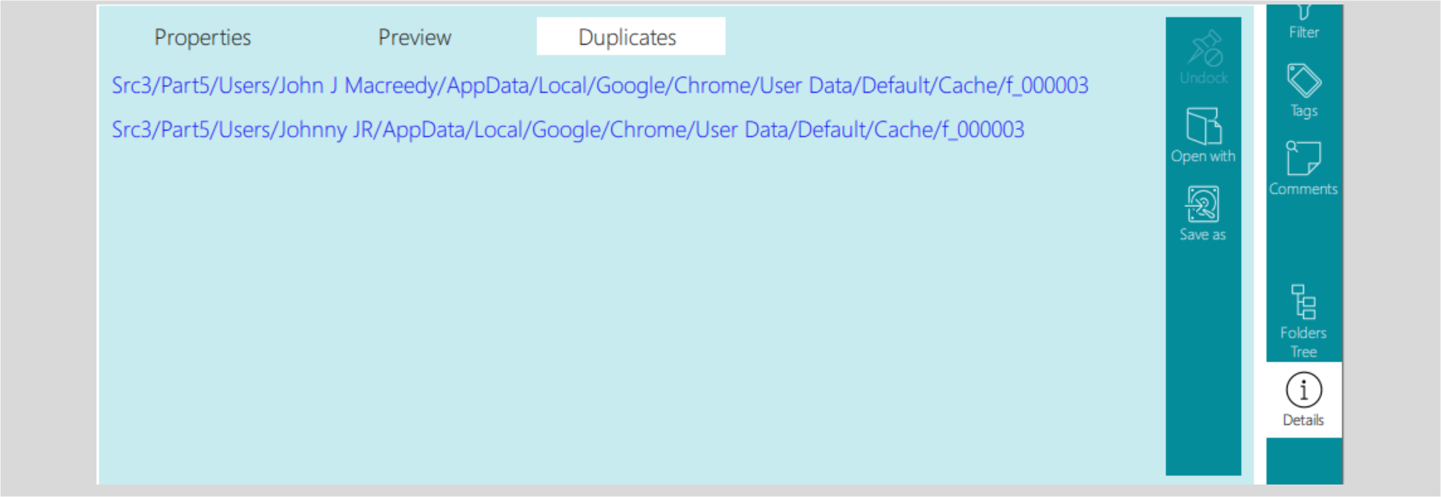
Deduplicating Files

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.



Src3/Part5/Users/John J Macreedy/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000003

Src3/Part5/Users/Johnny JR/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000003

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
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.
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 record for the downloaded file and to any file Captures that have collected the file concerned.

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.
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.
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.
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.

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.

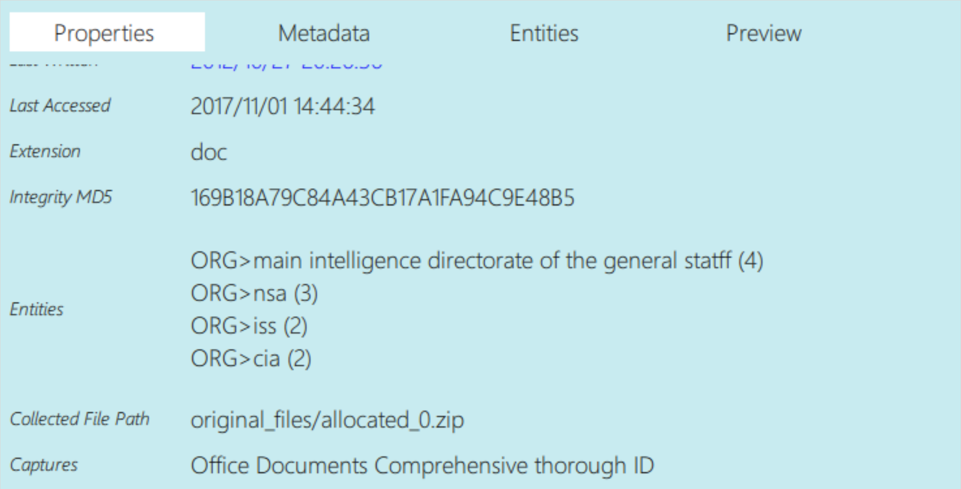
The Match indicator can also be used to sort and filter records.

Entities Property

This section applies to the following applications				
Rosoka Add-on				

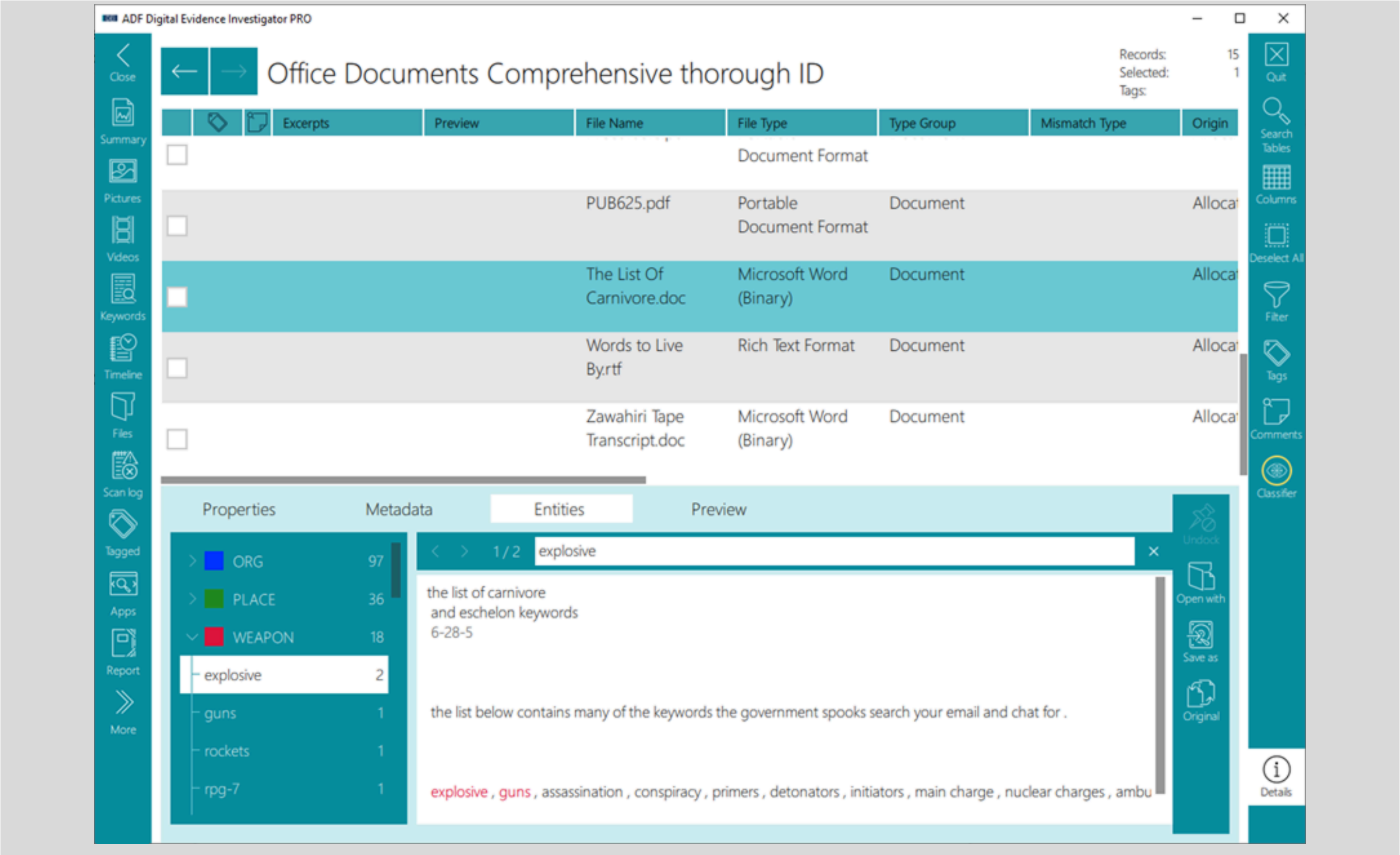
Entities are words of a document that represent a person, a place, an organization, a timestamp, and many more concepts (there are close to 50 different types of entity that can be identified). The Rosoka Add-on can find entities in more than 200 different languages and can translate them back into English.

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:



Last Accessed	2017/11/01 14:44:34
Extension	doc
Integrity MD5	169B18A79C84A43CB17A1FA94C9E48B5
Entities	ORG>main intelligence directorate of the general statff (4) ORG>nsa (3) ORG>iss (2) ORG>cia (2)
Collected File Path	original_files/allocated_0.zip
Captures	Office Documents Comprehensive thorough ID

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



Office Documents Comprehensive thorough ID

Records: 15
Selected: 1
Tags:

			Excerpts	Preview	File Name	File Type	Type Group	Mismatch Type	Origin
□						Document Format			
□					PUB625.pdf	Portable Document Format	Document		Allocat
□					The List Of Carnivore.doc	Microsoft Word (Binary)	Document		Allocat
□					Words to Live By.rtf	Rich Text Format	Document		Allocat
□					Zawahiri Tape Transcript.doc	Microsoft Word (Binary)	Document		Allocat

🟦	ORG	97
🟩	PLACE	36
🟥	WEAPON	18
	explosive	2
	guns	1
	rockets	1
	rpg-7	1

1 / 2 explosive

the list of carnivore
and eschelon keywords
6-28-5

the list below contains many of the keywords the government spooks search your email and chat for .

explosive , guns , assassination , conspiracy , primers , detonators , initiators , main charge , nuclear charges , ambu

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.

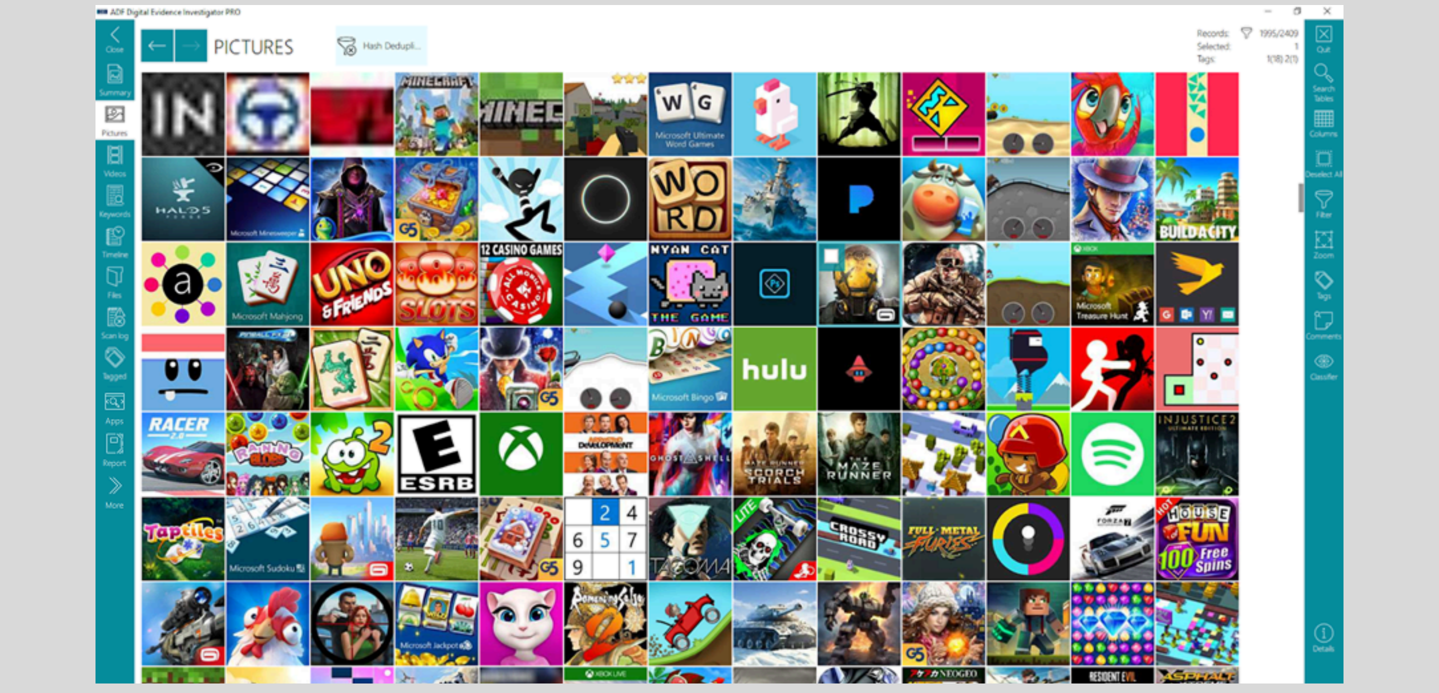
The **Entities** tab shows the following:

- 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.

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.



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.
🗒	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.

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

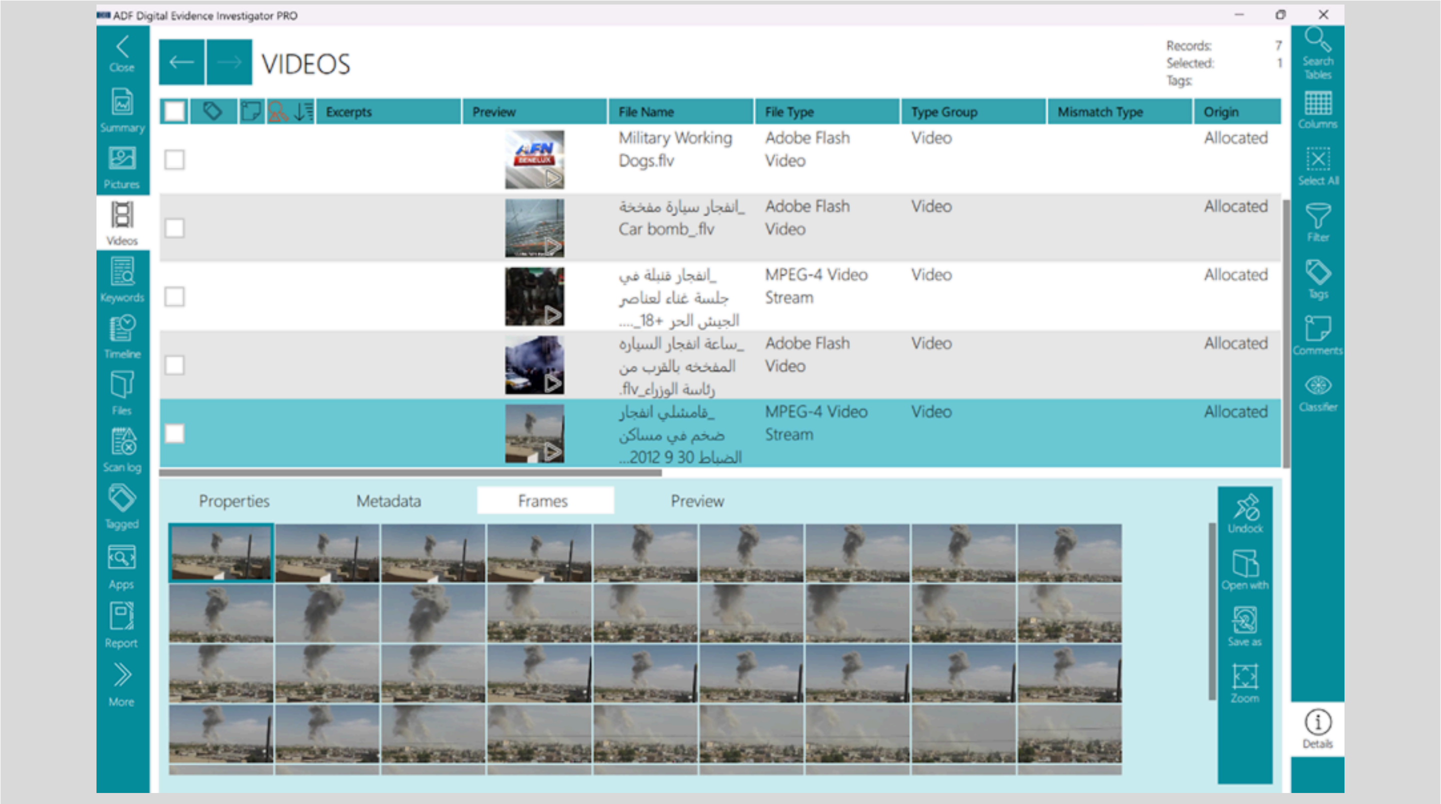
Photo Probability filtering is applicable to all pictures within the Picture File Types group. The Photo Probability score indicates how likely it is that the file is a photograph. Files with a score lower than 70% are very unlikely to be a photograph and more likely to be other picture types such as 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%.

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.



VIDEOS

Records: 7
Selected: 1
Tags:

□	Excerpts	Preview	File Name	File Type	Type Group	Mismatch Type	Origin
□			Military Working Dogs.flv	Adobe Flash Video	Video		Allocated
□			_انفجار سيارة مفخخة Car bomb_.flv	Adobe Flash Video	Video		Allocated
□			_انفجار قنبلة في جلسة غناء لعناصر الجيش الحر +18_....	MPEG-4 Video Stream	Video		Allocated
□			_ساعة انفجار السياره المفخخه بالقرب من رئاسة الوزراء_flv.	Adobe Flash Video	Video		Allocated
□			_قامشلي انفجار ضخم في مساكن الضباط 30 9 2012...	MPEG-4 Video Stream	Video		Allocated

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.
▷	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

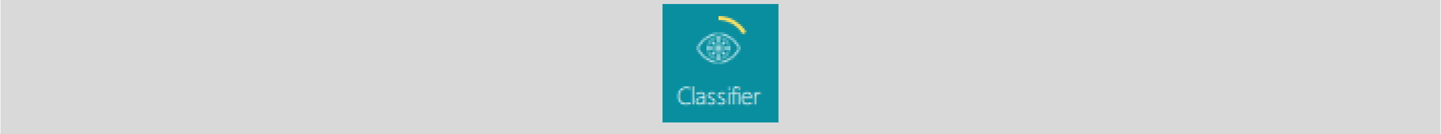
Open the Details panel on the Frames tab and use the keyboard arrow down to navigate through the videos one at a time.

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 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 + 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

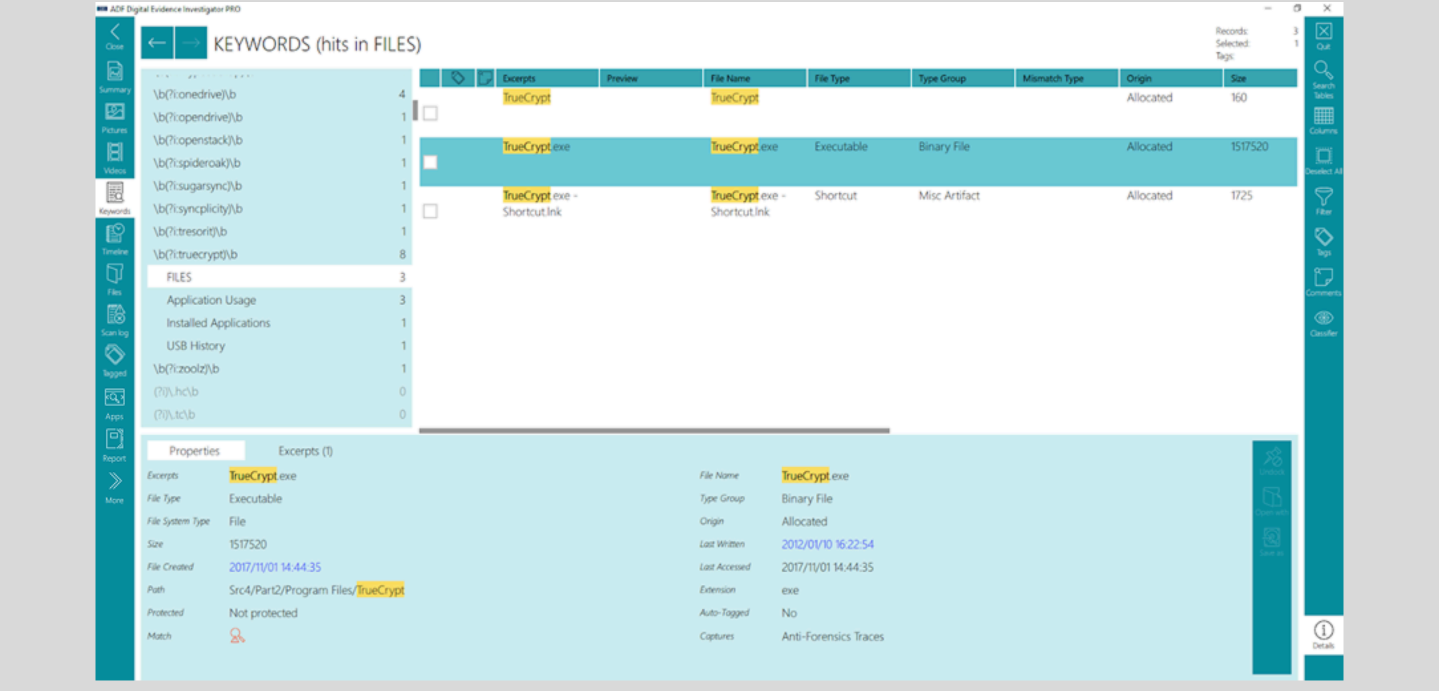
This process is only available in the Desktop application and not during a live or boot scan.

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 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.



KEYWORDS (hits in FILES)

Records: 3
Selected: 1
Tags:

\b(?i:onedrive)\b	4
\b(?i:opendrive)\b	1
\b(?i:openstack)\b	1
\b(?i:spideroak)\b	1
\b(?i:sugarsync)\b	1
\b(?i:syncplicity)\b	1
\b(?i:tresorit)\b	1
\b(?i:truecrypt)\b	8
FILES	3
Application Usage	3
Installed Applications	1
USB History	1
\b(?i:zoolz)\b	1
(?i)\.hc\b	0
(?i)\.tc\b	0

			Excerpts	Preview	File Name	File Type	Type Group	Mismatch Type	Origin	Size
□			TrueCrypt		TrueCrypt				Allocated	160
□			TrueCrypt.exe		TrueCrypt.exe	Executable	Binary File		Allocated	1517520
□			TrueCrypt.exe - Shortcut.lnk		TrueCrypt.exe - Shortcut.lnk	Shortcut	Misc Artifact		Allocated	1725

Properties Excerpts (1)

Excerpts	TrueCrypt.exe	File Name	TrueCrypt.exe
File Type	Executable	Type Group	Binary File
File System Type	File	Origin	Allocated
Size	1517520	Last Written	2012/01/10 16:22:54
File Created	2017/11/01 14:44:35	Last Accessed	2017/11/01 14:44:35
Path	Src4/Part2/Program Files/TrueCrypt	Extension	exe
Protected	Not protected	Auto-Tagged	No
Match		Captures	Anti-Forensics Traces

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”

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	Y	Y	Y

	activity			
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.

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
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
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: - Allocated: files that are accessible to the user via the file system - Embedded: files contained within another file (usually archives or cache containers) - Unallocated: files no longer referenced by the file system for which the data can still be found on consecutive sectors	Y	Y	Y

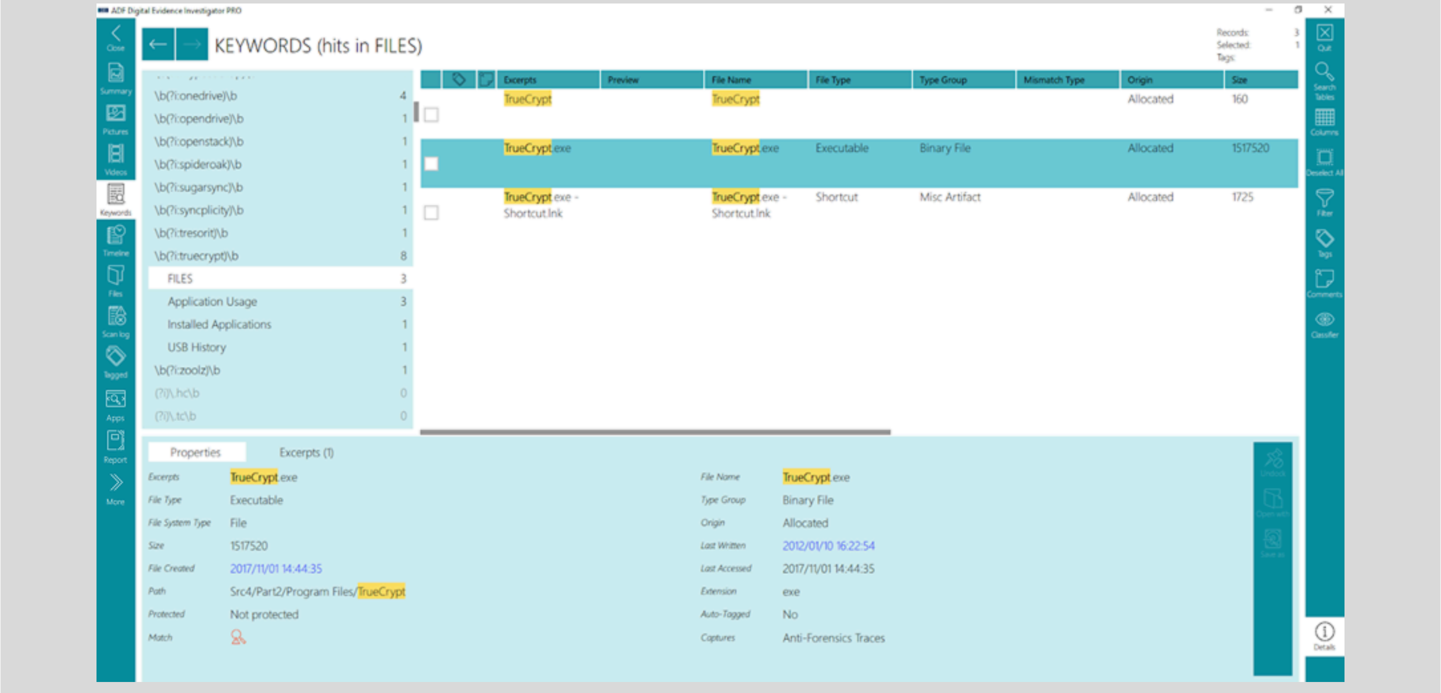
	- Deleted: files that are still referenced by the file system but marked as deleted and for which the sectors are reusable - Inaccessible: files that are locked and cannot be read			
Accessible	Possible values are: - True: the content of the file is accessible. - False: the content of the file was inaccessible and only file system metadata were available.	Y	Y	Y
File Size	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
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 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,		Y	Y

	100 extremely likely)			
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
Match	Set to true if that file was matched by hash value or keywords		Y	Y
Captures	Capture names that processed and matched that file			Y
PhotoDNA Score	Indicates how visually similar this picture is from a picture in a PhotoDNA Capture. Zero is the most visually similar. The absolute score value cannot be interpreted and should only be used to order records		Y	Y

Scan Log View

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

- Error processing a file including the file name
- Limit reached (for example 50 keywords hits in the same file)
- Protected file encountered
- Scan progress information



KEYWORDS (hits in FILES)

Records: 3
Selected: 1
Tags:

\b(?i:onedrive)\b	4
\b(?i:opendrive)\b	1
\b(?i:openstack)\b	1
\b(?i:spideroak)\b	1
\b(?i:sugarsync)\b	1
\b(?i:syncplicity)\b	1
\b(?i:tresorit)\b	1
\b(?i:truecrypt)\b	8
FILES	3
Application Usage	3
Installed Applications	1
USB History	1
\b(?i:zoolz)\b	1
(?i)\.hc\b	0
(?i)\.tc\b	0

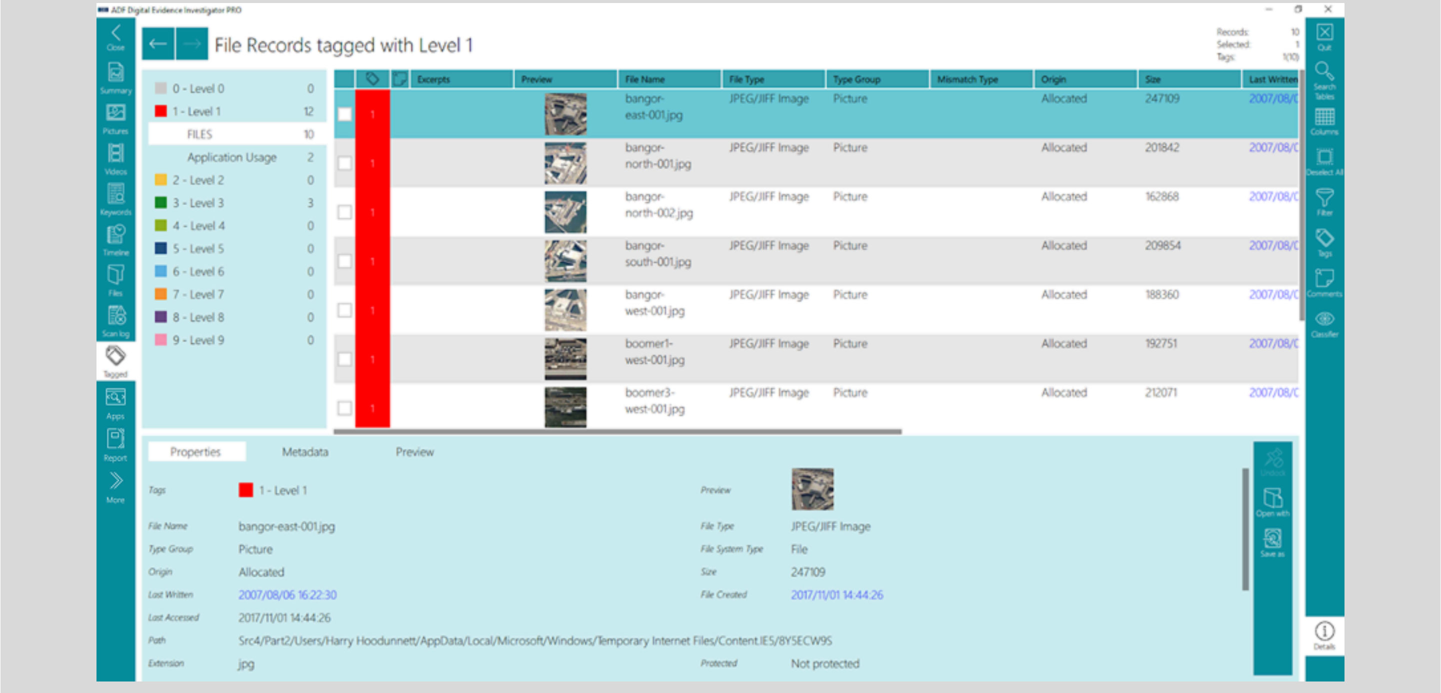
			Excerpts	Preview	File Name	File Type	Type Group	Mismatch Type	Origin	Size
□			TrueCrypt		TrueCrypt				Allocated	160
□			TrueCrypt.exe		TrueCrypt.exe	Executable	Binary File		Allocated	1517520
□			TrueCrypt.exe - Shortcut.lnk		TrueCrypt.exe - Shortcut.lnk	Shortcut	Misc Artifact		Allocated	1725

Properties Excerpts (1)

Excerpts	TrueCrypt.exe	File Name	TrueCrypt.exe
File Type	Executable	Type Group	Binary File
File System Type	File	Origin	Allocated
Size	1517520	Last Written	2012/01/10 16:22:54
File Created	2017/11/01 14:44:35	Last Accessed	2017/11/01 14:44:35
Path	Src4/Part2/Program Files/TrueCrypt	Extension	exe
Protected	Not protected	Auto-Tagged	No
Match		Captures	Anti-Forensics Traces

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.



File Records tagged with Level 1

Records: 10
Selected: 1
Tags: 1(10)

⬜ 0 - Level 0	0
🟥 1 - Level 1	12
FILES	10
Application Usage	2
🟨 2 - Level 2	0
🟩 3 - Level 3	3
🟩 4 - Level 4	0
🟦 5 - Level 5	0
🟦 6 - Level 6	0
🟧 7 - Level 7	0
🟪 8 - Level 8	0
🟥 9 - Level 9	0

			Excerpts	Preview	File Name	File Type	Type Group	Mismatch Type	Origin	Size	Last Written
□	1				bangor-east-001.jpg	JPEG/JIFF Image	Picture		Allocated	247109	2007/08/(
□	1				bangor-north-001.jpg	JPEG/JIFF Image	Picture		Allocated	201842	2007/08/(
□	1				bangor-north-002.jpg	JPEG/JIFF Image	Picture		Allocated	162868	2007/08/(
□	1				bangor-south-001.jpg	JPEG/JIFF Image	Picture		Allocated	209854	2007/08/(
□	1				bangor-west-001.jpg	JPEG/JIFF Image	Picture		Allocated	188360	2007/08/(
□	1				boomer1-west-001.jpg	JPEG/JIFF Image	Picture		Allocated	192751	2007/08/(
□	1				boomer3-west-001.jpg	JPEG/JIFF Image	Picture		Allocated	212071	2007/08/(

Properties Metadata Preview

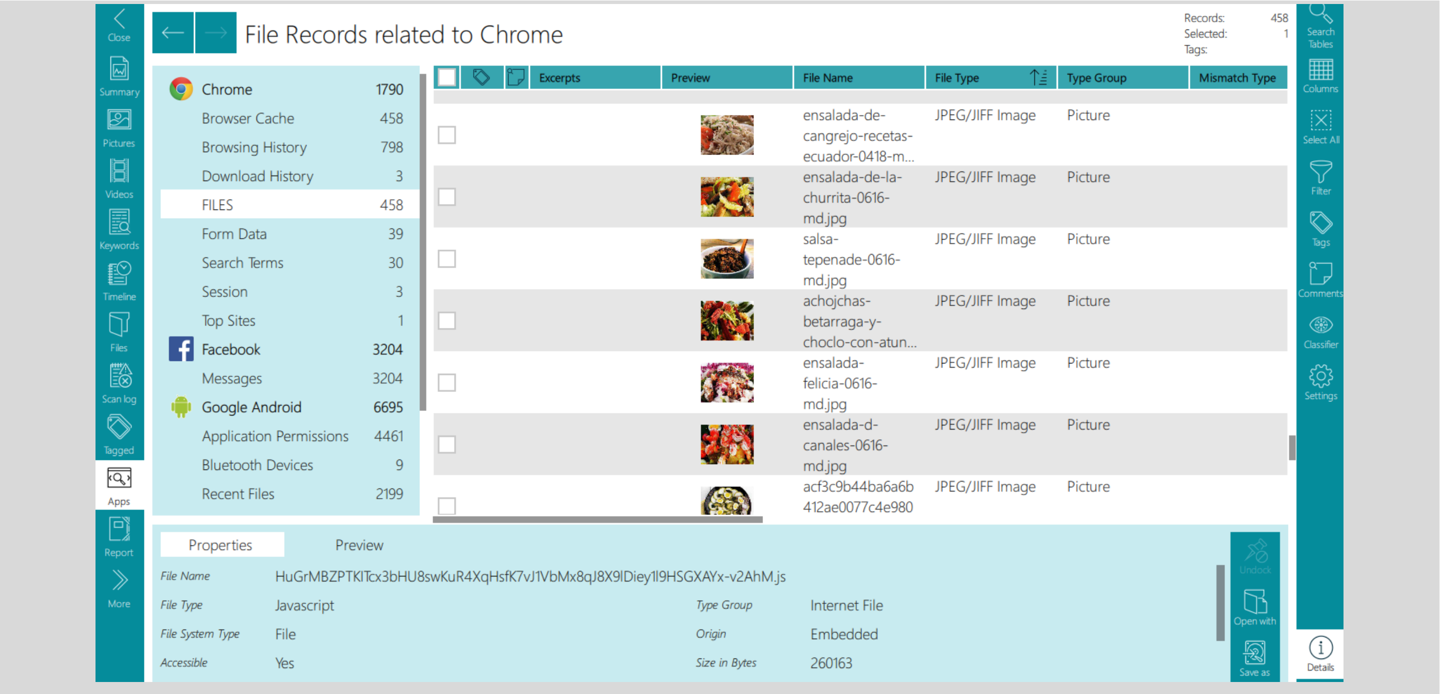
Tags	🟥 1 - Level 1	Preview	
File Name	bangor-east-001.jpg	File Type	JPEG/JIFF Image
Type Group	Picture	File System Type	File
Origin	Allocated	Size	247109
Last Written	2007/08/06 16:22:30	File Created	2017/11/01 14:44:26
Last Accessed	2017/11/01 14:44:26		
Path	Src4/Part2/Users/Harry Hoodunnett/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/8Y5ECW9S		
Extension	jpg	Protected	Not protected

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.



File Records related to Chrome

Records: 458
Selected: 1
Tags:

Chrome	1790
Browser Cache	458
Browsing History	798
Download History	3
FILES	458
Form Data	39
Search Terms	30
Session	3
Top Sites	1
Facebook	3204
Messages	3204
Google Android	6695
Application Permissions	4461
Bluetooth Devices	9
Recent Files	2199

□			Excerpts	Preview	File Name	File Type	Type Group	Mismatch Type
□					ensalada-de-cangrejo-recetas-ecuador-0418-m...	JPEG/JIFF Image	Picture	
□					ensalada-de-la-churrita-0616-md.jpg	JPEG/JIFF Image	Picture	
□					salsa-tepenade-0616-md.jpg	JPEG/JIFF Image	Picture	
□					achojchas-betarraga-y-choclo-con-atun...	JPEG/JIFF Image	Picture	
□					ensalada-felicia-0616-md.jpg	JPEG/JIFF Image	Picture	
□					ensalada-d-canales-0616-md.jpg	JPEG/JIFF Image	Picture	
□					acf3c9b44ba6a6b412ae0077c4e980	JPEG/JIFF Image	Picture	

Properties Preview

File Name	HuGrMBZPTKITcx3bHU8swKuR4XqHsfK7vJ1VbMx8qJ8X9lDiey1l9HSGXAYx-v2AhM.js		
File Type	Javascript	*Type Group*	Internet File
File System Type	File	*Origin*	Embedded
Accessible	Yes	*Size in Bytes*	260163

Capture Views

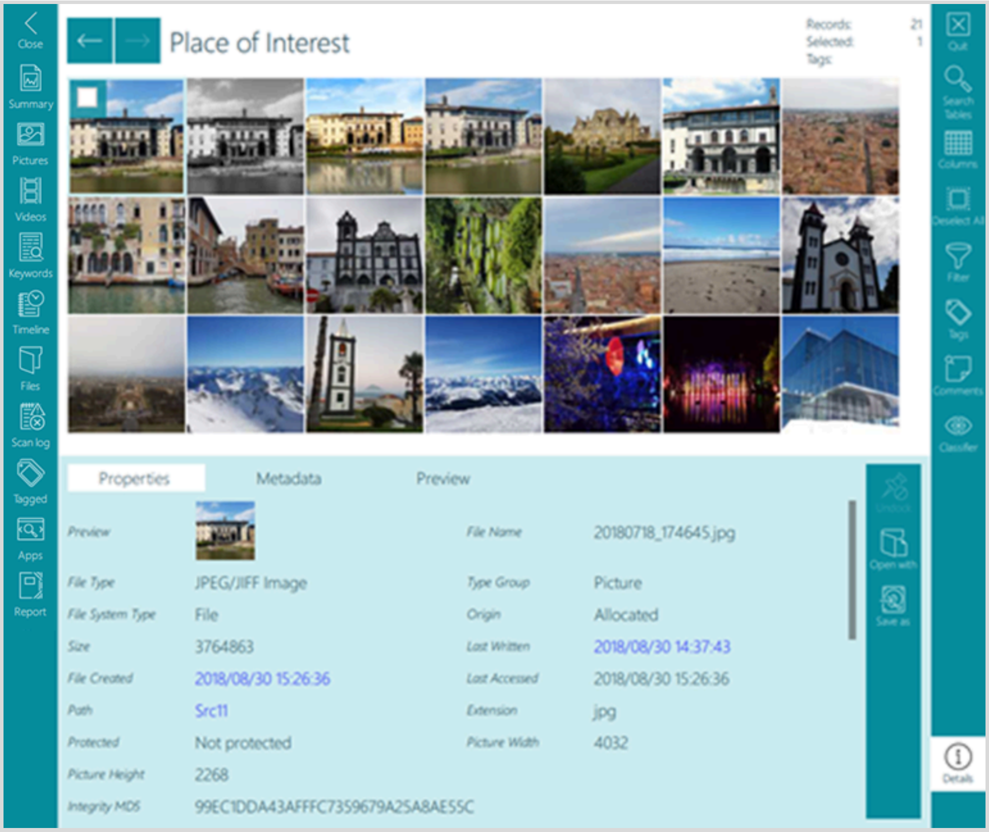
The Capture views show the records collected by each Capture.

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.



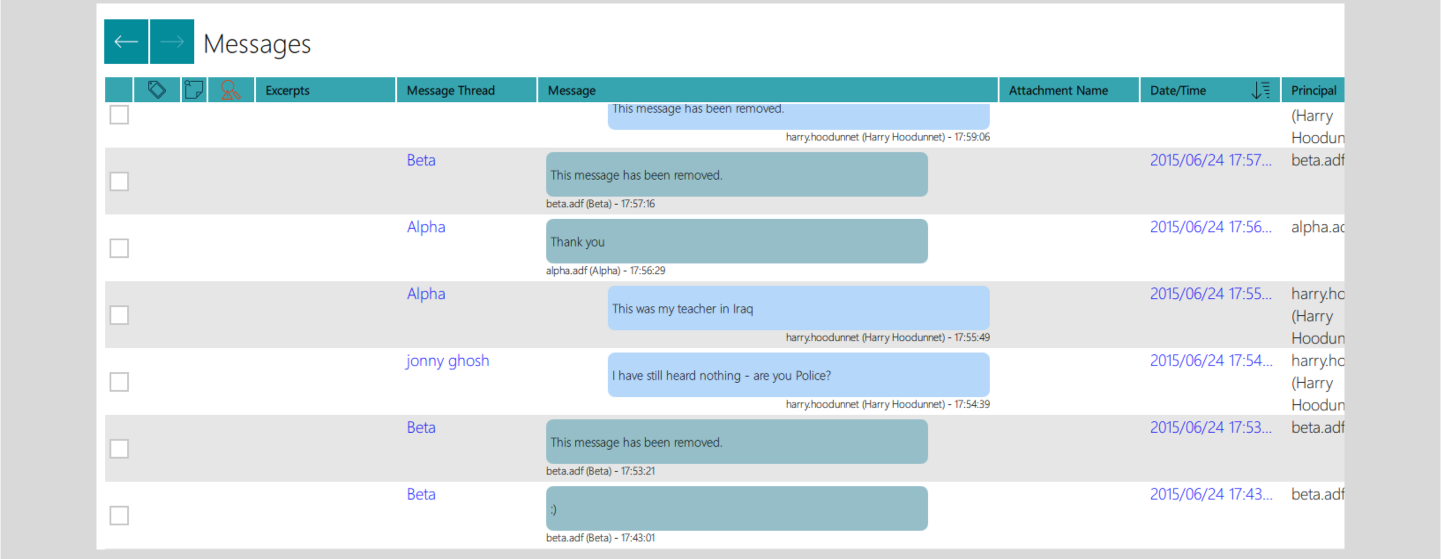
Place of Interest

Records: 21
Selected: 1
Tags:

Preview
File Name 20180718_174645.jpg
File Type JPEG/JIFF Image
Type Group Picture
File System Type File
Origin Allocated
Size 3764863
Last Written 2018/08/30 14:37:43
File Created 2018/08/30 15:26:36
Last Accessed 2018/08/30 15:26:36
Path Src11
Extension jpg
Protected Not protected
Picture Width 4032
Picture Height 2268
Integrity MD5 99EC1DDA43AFFFC7359679A25A8AE55C

Messages View

The Messages artifact Captures displays messages collected in Chat applications.



Messages

				Excerpts	Message Thread	Message	Attachment Name	Date/Time	Principal
□						This message has been removed. harry.hoodunnet (Harry Hoodunnet) - 17:59:06			(Harry Hoodun
□					Beta	This message has been removed. beta.adf (Beta) - 17:57:16		2015/06/24 17:57...	beta.adf
□					Alpha	Thank you alpha.adf (Alpha) - 17:56:29		2015/06/24 17:56...	alpha.ad
□					Alpha	This was my teacher in Iraq harry.hoodunnet (Harry Hoodunnet) - 17:55:49		2015/06/24 17:55...	harry.ho (Harry Hoodun
□					jonny ghosh	I have still heard nothing - are you Police? harry.hoodunnet (Harry Hoodunnet) - 17:54:39		2015/06/24 17:54...	harry.ho (Harry Hoodun
□					Beta	This message has been removed. beta.adf (Beta) - 17:53:21		2015/06/24 17:53...	beta.adf
□					Beta	:) beta.adf (Beta) - 17:43:01		2015/06/24 17:43...	beta.adf

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.

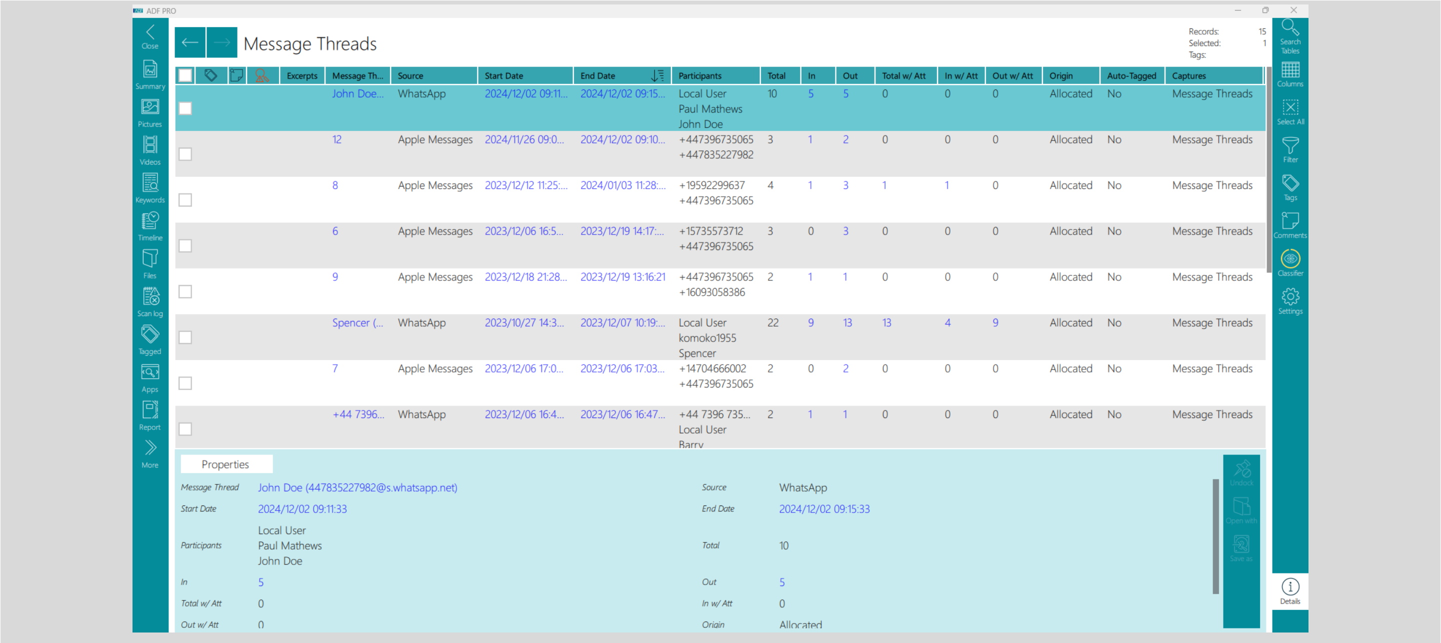
If a message started with "ADF NOTE" it means that the content was edited by the ADF application to provide more context.

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.



Message Threads

Records: 15
Selected: 1
Tags:

□				Excerpts	Message Th...	Source	Start Date	End Date	Participants	Total	In	Out	Total w/ Att	In w/ Att	Out w/ Att	Origin	Auto-Tagged	Captures
□					John Doe...	WhatsApp	2024/12/02 09:11...	2024/12/02 09:15...	Local User Paul Mathews John Doe	10	5	5	0	0	0	Allocated	No	Message Threads
□					12	Apple Messages	2024/11/26 09:0...	2024/12/02 09:10...	+447396735065 +447835227982	3	1	2	0	0	0	Allocated	No	Message Threads
□					8	Apple Messages	2023/12/12 11:25:...	2024/01/03 11:28:...	+19592299637 +447396735065	4	1	3	1	1	0	Allocated	No	Message Threads
□					6	Apple Messages	2023/12/06 16:5...	2023/12/19 14:17:...	+15735573712 +447396735065	3	0	3	0	0	0	Allocated	No	Message Threads
□					9	Apple Messages	2023/12/18 21:28...	2023/12/19 13:16:21	+447396735065 +16093058386	2	1	1	0	0	0	Allocated	No	Message Threads
□					Spencer (...	WhatsApp	2023/10/27 14:3...	2023/12/07 10:19:...	Local User komoko1955 Spencer	22	9	13	13	4	9	Allocated	No	Message Threads
□					7	Apple Messages	2023/12/06 17:0...	2023/12/06 17:03...	+14704666002 +447396735065	2	0	2	0	0	0	Allocated	No	Message Threads
□					+44 7396...	WhatsApp	2023/12/06 16:4...	2023/12/06 16:47...	+44 7396 735... Local User Barry	2	1	1	0	0	0	Allocated	No	Message Threads

Properties

Message Thread	John Doe (447835227982@s.whatsapp.net)	*Source*	WhatsApp
Start Date	2024/12/02 09:11:33	*End Date*	2024/12/02 09:15:33
Participants	Local User Paul Mathews John Doe	*Total*	10
In	5	*Out*	5
Total w/ Att	0	*In w/ Att*	0
Out w/ Att	0	*Origin*	Allocated

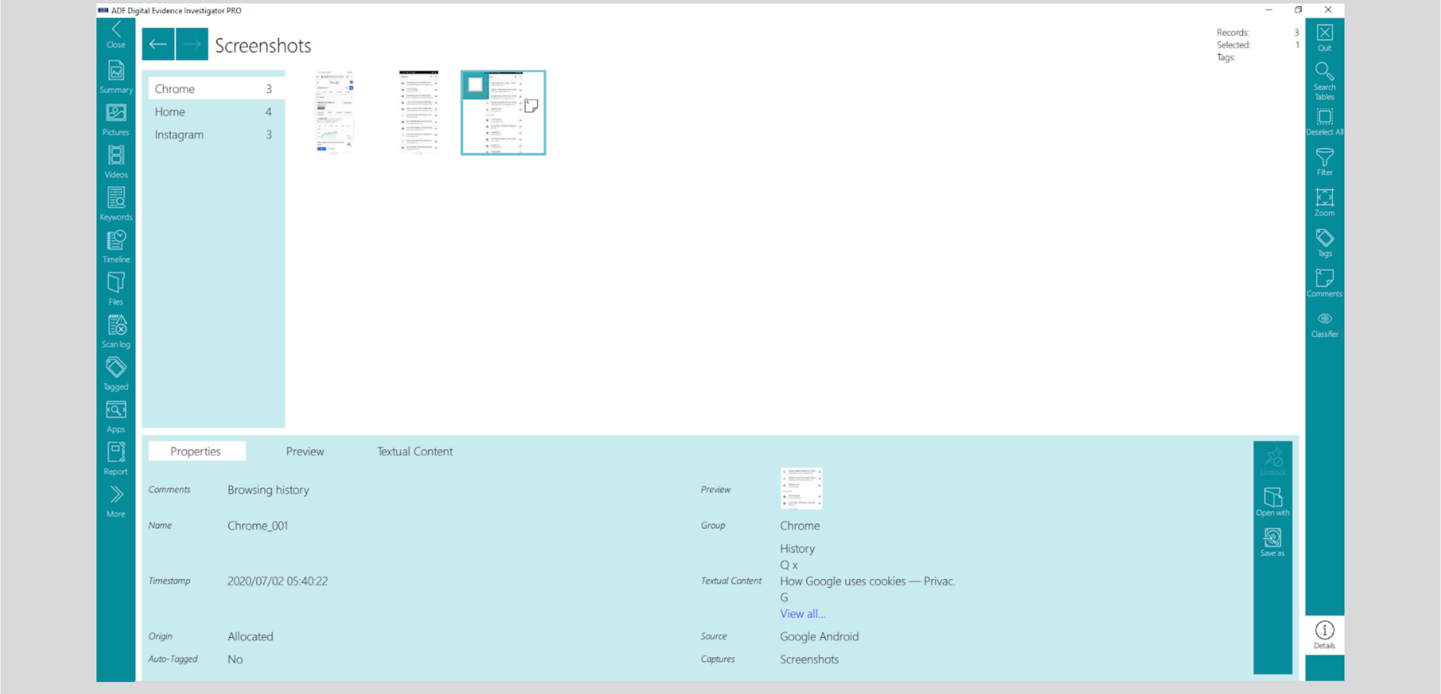
Table columns

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. Displayed as a hyperlink to the Messages view, filtered to show only incoming messages.
Out	Number of messages sent by the local user. Displayed as a hyperlink to the Messages view,

	filtered to show only outgoing messages.
Total w/ Att	Number of messages that include attachments. Displayed as a hyperlink to the Messages view, filtered to show messages containing attachments.
In w/ Att	Number of incoming messages containing attachments. Displayed as a hyperlink to the Messages view, filtered to show incoming messages with attachments.
Out w/ Att	Number of outgoing messages containing attachments. Displayed as a hyperlink to the Messages view, filtered to show outgoing messages with attachments.

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.



Records: 3
Selected: 1
Tags:

Chrome	3
Home	4
Instagram	3

Comments: Browsing history
Name: Chrome_001
Timestamp: 2020/07/02 05:40:22
Origin: Allocated
Auto-Tagged: No
Preview:
Group: Chrome
Textual Content: History
Q x
How Google uses cookies — Privac.
G
View all...
Source: Google Android
Captures: Screenshots

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.

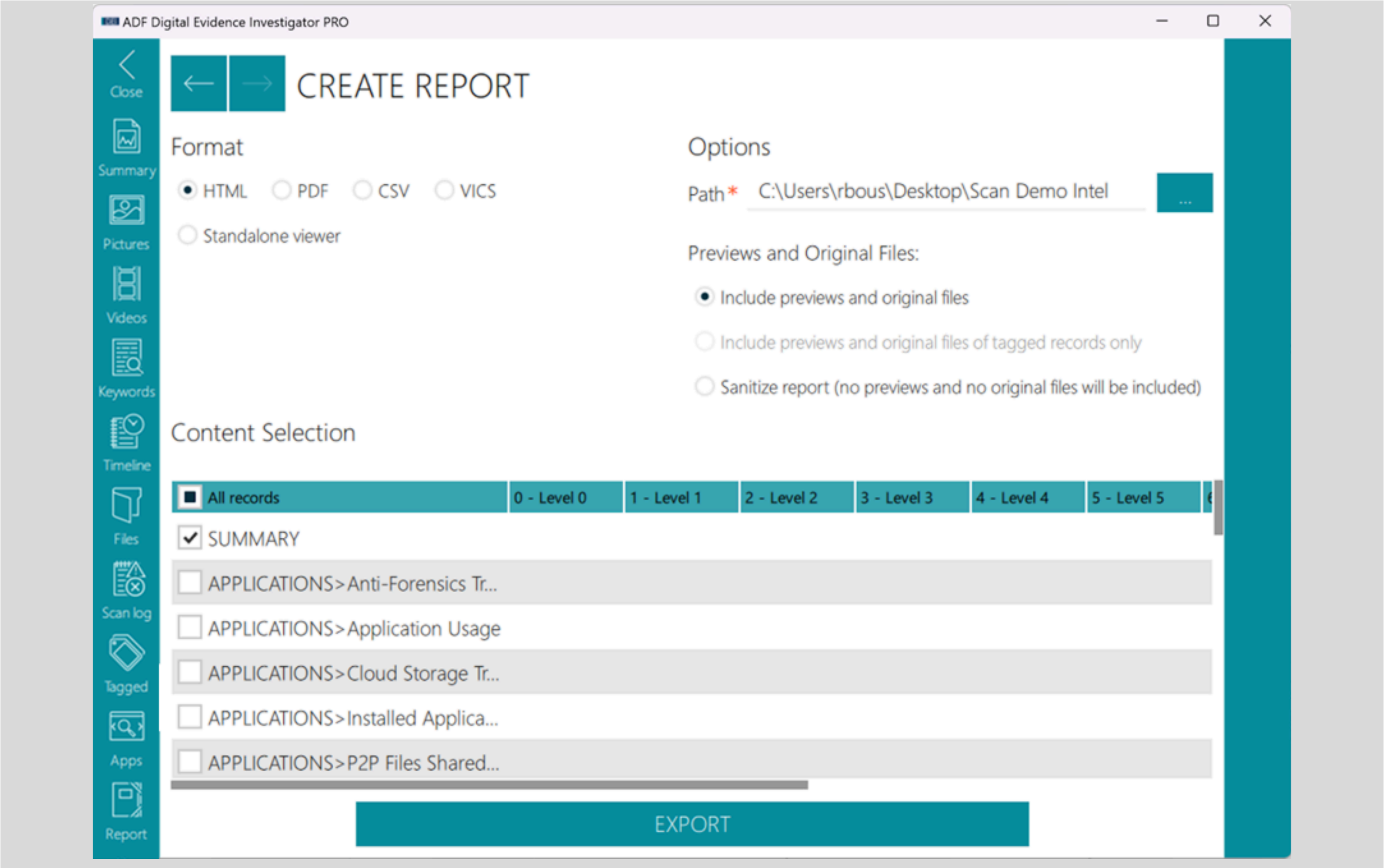
Note that the tabs of the Details panel are adjusted based on the selected item type.

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 PRO).

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.



CREATE REPORT

Format

● HTML ○ PDF ○ CSV ○ VICS

○ Standalone viewer

Options

Path* C:\Users\rbous\Desktop\Scan Demo Intel

Previews and Original Files:

● Include previews and original files

○ Include previews and original files of tagged records only

○ Sanitize report (no previews and no original files will be included)

Content Selection

■ All records	0 - Level 0	1 - Level 1	2 - Level 2	3 - Level 3	4 - Level 4	5 - Level 5
☑ SUMMARY						
□ APPLICATIONS>Anti-Forensics Tr...						
□ APPLICATIONS>Application Usage						
□ APPLICATIONS>Cloud Storage Tr...						
□ APPLICATIONS>Installed Applica...						
□ APPLICATIONS>P2P Files Shared...						

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.

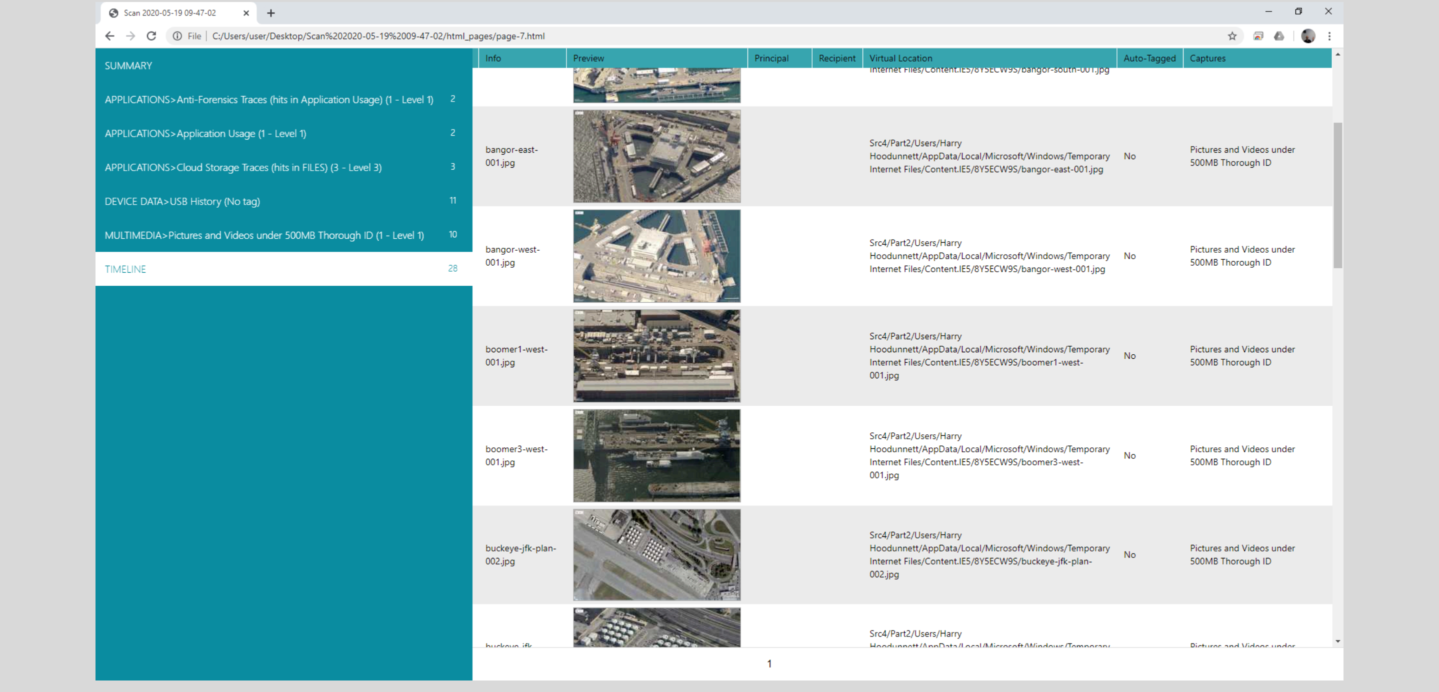
HTML Report

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

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.


Scan 2020-05-19 09-47-02
File
C:/Users/user/Desktop/Scan%202020-05-19%2009-47-02/html_pages/page-7.html

SUMMARY	
APPLICATIONS>Anti-Forensics Traces (hits in Application Usage) (1 - Level 1)	2
APPLICATIONS>Application Usage (1 - Level 1)	2
APPLICATIONS>Cloud Storage Traces (hits in FILES) (3 - Level 3)	3
DEVICE DATA>USB History (No tag)	11
MULTIMEDIA>Pictures and Videos under 500MB Thorough ID (1 - Level 1)	10
TIMELINE	28

Info	Preview	Principal	Recipient	Virtual Location	Auto-Tagged	Captures
				Internet Files/Content.IE5/8Y5ECW9S/bangor-south-001.jpg		
bangor-east-001.jpg				Src4/Part2/Users/Harry Hoodunnett/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/8Y5ECW9S/bangor-east-001.jpg	No	Pictures and Videos under 500MB Thorough ID
bangor-west-001.jpg				Src4/Part2/Users/Harry Hoodunnett/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/8Y5ECW9S/bangor-west-001.jpg	No	Pictures and Videos under 500MB Thorough ID
boomer1-west-001.jpg				Src4/Part2/Users/Harry Hoodunnett/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/8Y5ECW9S/boomer1-west-001.jpg	No	Pictures and Videos under 500MB Thorough ID
boomer3-west-001.jpg				Src4/Part2/Users/Harry Hoodunnett/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/8Y5ECW9S/boomer3-west-001.jpg	No	Pictures and Videos under 500MB Thorough ID
buckeye-jfk-plan-002.jpg				Src4/Part2/Users/Harry Hoodunnett/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/8Y5ECW9S/buckeye-jfk-plan-002.jpg	No	Pictures and Videos under 500MB Thorough ID
buckeye-jfk				Src4/Part2/Users/Harry Hoodunnett/AppData/Local/Microsoft/Windows/Temporary		Pictures and Videos under

PDF Report

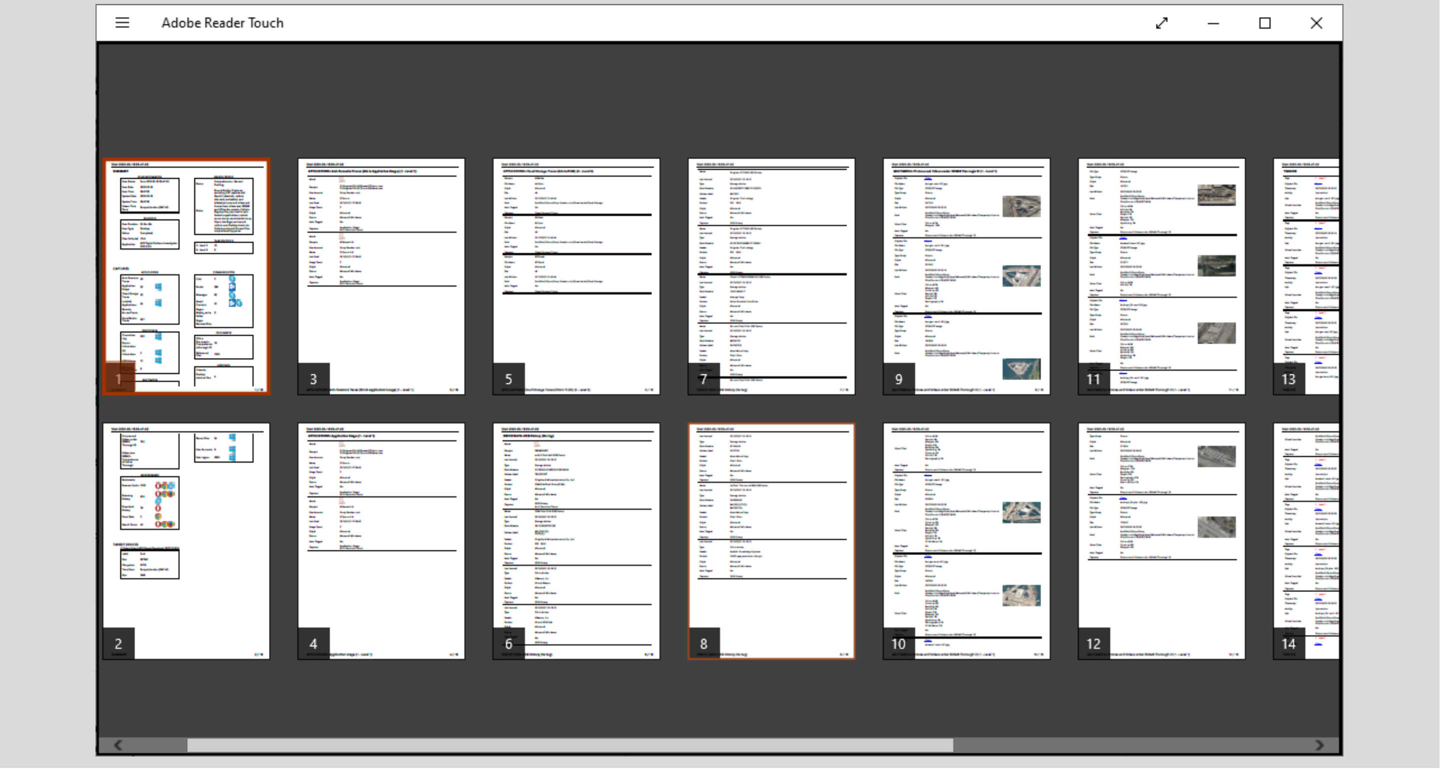
To create a PDF report that can be opened by Acrobat Reader or another PDF viewer, select the PDF format, select the destination folder, select the orientation (landscape or portrait), select the content, and click on the EXPORT button.

> 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.



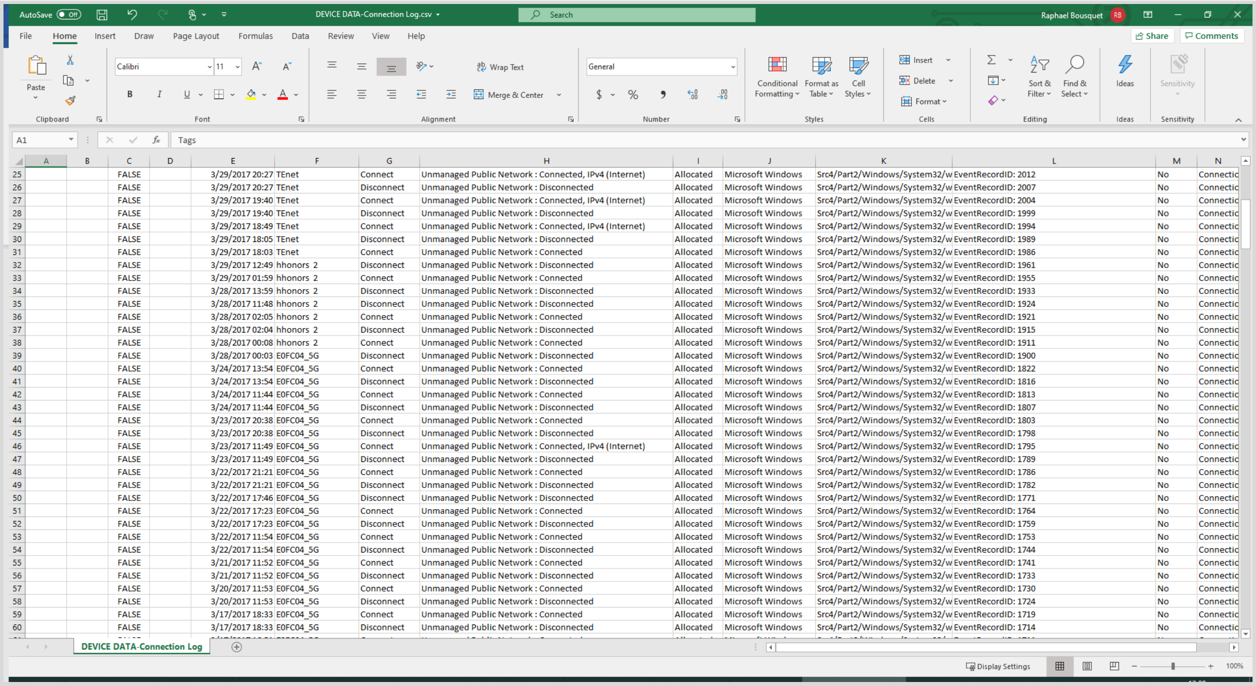
CSV Report

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.



A1 Tags

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
25			FALSE		3/29/2017 20:27	TEnet	Connect	Unmanaged Public Network : Connected, IPv4 (Internet)	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 2012	No	Connectic
26			FALSE		3/29/2017 20:27	TEnet	Disconnect	Unmanaged Public Network : Disconnected	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 2007	No	Connectic
27			FALSE		3/29/2017 19:40	TEnet	Connect	Unmanaged Public Network : Connected, IPv4 (Internet)	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 2004	No	Connectic
28			FALSE		3/29/2017 19:40	TEnet	Disconnect	Unmanaged Public Network : Disconnected	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1999	No	Connectic
29			FALSE		3/29/2017 18:49	TEnet	Connect	Unmanaged Public Network : Connected, IPv4 (Internet)	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1994	No	Connectic
30			FALSE		3/29/2017 18:05	TEnet	Disconnect	Unmanaged Public Network : Disconnected	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1989	No	Connectic
31			FALSE		3/29/2017 18:03	TEnet	Connect	Unmanaged Public Network : Connected	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1986	No	Connectic
32			FALSE		3/29/2017 12:49	hhonors 2	Disconnect	Unmanaged Public Network : Disconnected	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1961	No	Connectic
33			FALSE		3/29/2017 01:59	hhonors 2	Connect	Unmanaged Public Network : Connected	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1955	No	Connectic
34			FALSE		3/28/2017 13:59	hhonors 2	Disconnect	Unmanaged Public Network : Disconnected	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1933	No	Connectic
35			FALSE		3/28/2017 11:48	hhonors 2	Disconnect	Unmanaged Public Network : Disconnected	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1924	No	Connectic
36			FALSE		3/28/2017 02:05	hhonors 2	Connect	Unmanaged Public Network : Connected	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1921	No	Connectic
37			FALSE		3/28/2017 02:04	hhonors 2	Disconnect	Unmanaged Public Network : Disconnected	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1915	No	Connectic
38			FALSE		3/28/2017 00:08	hhonors 2	Connect	Unmanaged Public Network : Connected	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1911	No	Connectic
39			FALSE		3/28/2017 00:03	E0FC04_5G	Disconnect	Unmanaged Public Network : Disconnected	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1900	No	Connectic
40			FALSE		3/24/2017 13:54	E0FC04_5G	Connect	Unmanaged Public Network : Connected	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1822	No	Connectic
41			FALSE		3/24/2017 13:54	E0FC04_5G	Disconnect	Unmanaged Public Network : Disconnected	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1816	No	Connectic
42			FALSE		3/24/2017 11:44	E0FC04_5G	Connect	Unmanaged Public Network : Connected	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1813	No	Connectic
43			FALSE		3/24/2017 11:44	E0FC04_5G	Disconnect	Unmanaged Public Network : Disconnected	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1807	No	Connectic
44			FALSE		3/23/2017 20:38	E0FC04_5G	Connect	Unmanaged Public Network : Connected	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1803	No	Connectic
45			FALSE		3/23/2017 20:38	E0FC04_5G	Disconnect	Unmanaged Public Network : Disconnected	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1798	No	Connectic
46			FALSE		3/23/2017 11:49	E0FC04_5G	Connect	Unmanaged Public Network : Connected, IPv4 (Internet)	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1795	No	Connectic
47			FALSE		3/23/2017 11:49	E0FC04_5G	Disconnect	Unmanaged Public Network : Disconnected	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1789	No	Connectic
48			FALSE		3/22/2017 21:21	E0FC04_5G	Connect	Unmanaged Public Network : Connected	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1786	No	Connectic
49			FALSE		3/22/2017 21:21	E0FC04_5G	Disconnect	Unmanaged Public Network : Disconnected	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1782	No	Connectic
50			FALSE		3/22/2017 17:46	E0FC04_5G	Disconnect	Unmanaged Public Network : Disconnected	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1771	No	Connectic
51			FALSE		3/22/2017 17:23	E0FC04_5G	Connect	Unmanaged Public Network : Connected	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1764	No	Connectic
52			FALSE		3/22/2017 17:23	E0FC04_5G	Disconnect	Unmanaged Public Network : Disconnected	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1759	No	Connectic
53			FALSE		3/22/2017 11:54	E0FC04_5G	Connect	Unmanaged Public Network : Connected	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1753	No	Connectic
54			FALSE		3/22/2017 11:54	E0FC04_5G	Disconnect	Unmanaged Public Network : Disconnected	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1744	No	Connectic
55			FALSE		3/21/2017 11:52	E0FC04_5G	Connect	Unmanaged Public Network : Connected	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1741	No	Connectic
56			FALSE		3/21/2017 11:52	E0FC04_5G	Disconnect	Unmanaged Public Network : Disconnected	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1733	No	Connectic
57			FALSE		3/20/2017 11:53	E0FC04_5G	Connect	Unmanaged Public Network : Connected	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1730	No	Connectic
58			FALSE		3/20/2017 11:53	E0FC04_5G	Disconnect	Unmanaged Public Network : Disconnected	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1724	No	Connectic
59			FALSE		3/17/2017 18:33	E0FC04_5G	Connect	Unmanaged Public Network : Connected	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1719	No	Connectic
60			FALSE		3/17/2017 18:33	E0FC04_5G	Disconnect	Unmanaged Public Network : Disconnected	Allocated	Microsoft Windows	Src4/Part2/Windows/System32/w	EventRecordID: 1714	No	Connectic

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:

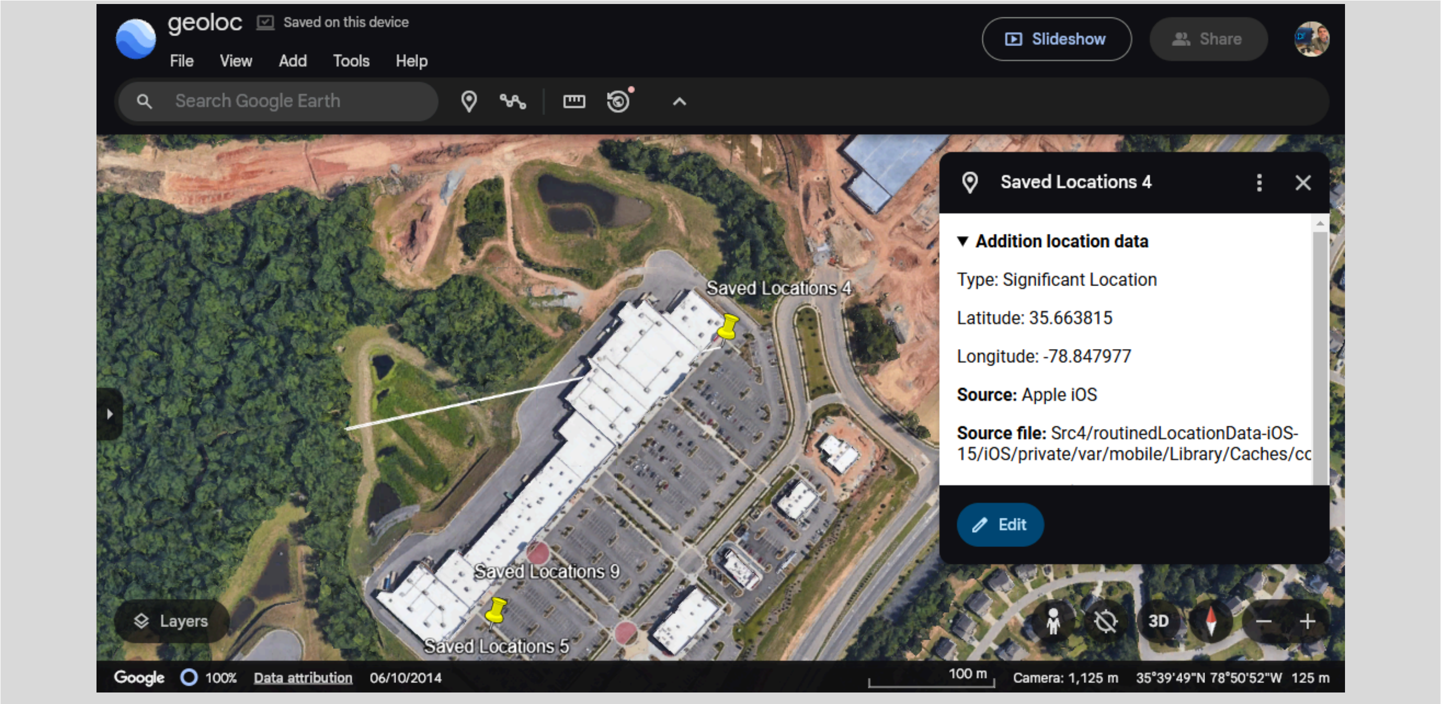
- Image Previews - where applicable, a visual preview of the associated file is included.
- EXIF Metadata - if available.
- File Name - the original name of the file.
- File Path - the file’s location within the source system.
- Source of the artifact when applicable.

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.

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

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



Saved Locations 4

▼ Addition location data

Type: Significant Location

Latitude: 35.663815

Longitude: -78.847977

Source: Apple iOS

Source file: Src4/routinedLocationData-iOS-15/iOS/private/var/mobile/Library/Caches/cc

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.

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.
Open	To open a scan result not located in the local ScanResults folder.
?	To open this guide.

Help	

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.