



## Standalone Report User Guide



Digital Evidence Investigator version 2.2



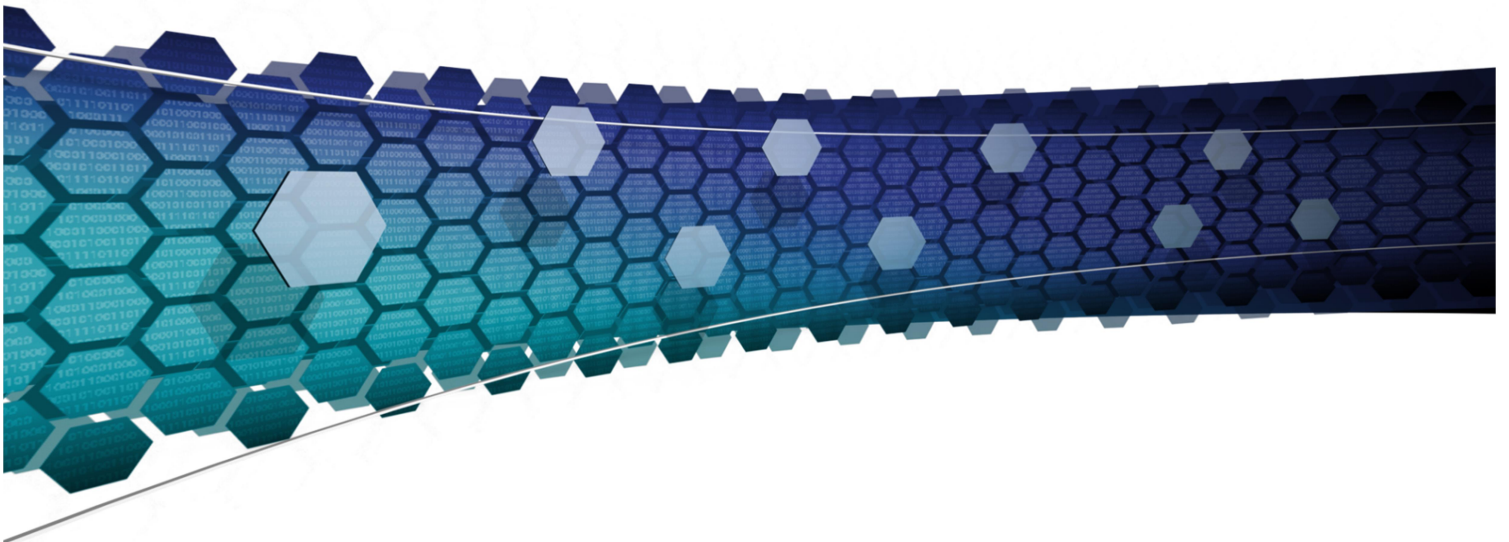
Triage Investigator version 5.2



Triage-G2 version 5.2



Mobile Device Investigator 2.2



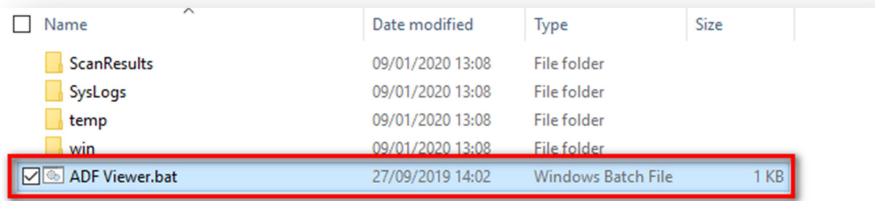
# Contents

1.	OPEN STANDALONE REPORT .....	3
2.	REVIEW SCAN RESULTS .....	4
	CAPTURE AND NAVIGATION TOOLBAR.....	4
	SUMMARY VIEW.....	7
	FUNCTION TOOLBARS .....	9
	DETAILS PANE .....	10
	FUNCTION TOOLBAR OF DETAILS PANE .....	11
	COLUMN CONTROLS .....	11
	FILTERING.....	12
	PHOTO PROBABILITY .....	17
	VISUAL CLASS.....	18
	SORTING .....	21
	RECORDS SELECTION AND NAVIGATION .....	21
	TAGGING.....	22
	COMMENTS.....	23
	SEARCH SCAN RESULTS .....	24
	TIMELINE .....	27
	FILES .....	29
	MESSAGES .....	30
	TAGGED VIEW.....	30
	DUPLICATE FILES.....	32
	REFERENCED FILE FUNCTIONALITY.....	33
	TIME ZONE SECTION.....	35
	REVIEWING SCREENSHOTS .....	36
3.	REPORTING.....	40
	HTML REPORT .....	41
	PDF REPORT .....	48
	CSV REPORT.....	50
	VICS REPORT.....	52

# 1. Open Standalone Report

A standalone report comprises the Scan Results from a case along with the ADF software to view these results. The standalone report folder looks like this:

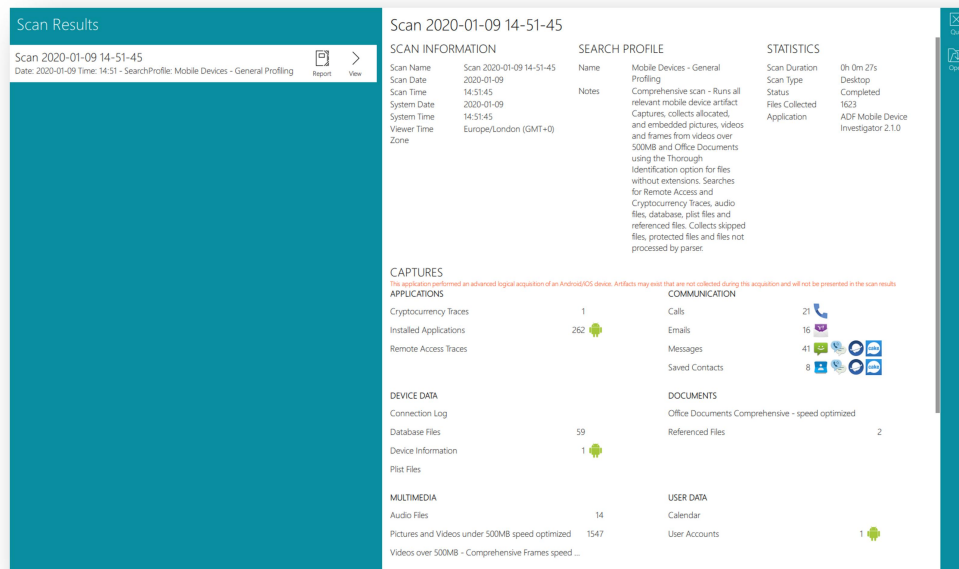
## Standalone Report Folder



Name	Date modified	Type	Size
ScanResults	09/01/2020 13:08	File folder	
SysLogs	09/01/2020 13:08	File folder	
temp	09/01/2020 13:08	File folder	
win	09/01/2020 13:08	File folder	
ADF Viewer.bat	27/09/2019 14:02	Windows Batch File	1 KB

Double clicking on the ADF Viewer.bat file opens the program into the Scan Results View:

## Scan Results View



Scan Results

Scan 2020-01-09 14-51-45

Date: 2020-01-09 Time: 14:51 - SearchProfile: Mobile Devices - General Profiling

Report View

Scan 2020-01-09 14-51-45

SCAN INFORMATION

Scan Name	Scan 2020-01-09 14-51-45
Scan Date	2020-01-09
Scan Time	14:51:45
System Date	2020-01-09
System Time	14:51:45
Viewer Time	Europe/London (GMT+0)
Zone	

SEARCH PROFILE

Name	Mobile Devices - General Profiling
Notes	Comprehensive scan - Runs all relevant mobile device artifacts. Captures, collects allocated, and embedded pictures, videos and frames from videos over 500MB and Office Documents using the Thorough Identification option for files without extensions. Searches for Remote Access and Cryptocurrency Traces, audio files, database, pilot files and referenced files. Collects skipped files, protected files and files not processed by parser.

STATISTICS

Scan Duration	0h 0m 27s
Scan Type	Desktop
Status	Completed
Files Collected	1623
Application	ADF-Mobile Device Investigator 2.1.0

CAPTURES

The 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

Cryptocurrency Traces	1
Installed Applications	262
Remote Access Traces	

COMMUNICATION

Calls	21
Emails	16
Messages	41
Saved Contacts	8

DEVICE DATA

Connection Log	
Database Files	59
Device Information	1
Plist Files	

MULTIMEDIA

Audio Files	14
Pictures and Videos under 500MB speed optimized	1547
Videos over 500MB - Comprehensive Frames speed ...	

DOCUMENTS

Office Documents Comprehensive - speed optimized	
Referenced Files	2

USER DATA

Calendar	
User Accounts	1







Clicking the View button will open the Scan to be reviewed.





The Function Toolbar contains two buttons. The Quit button will close the Standalone Viewer while the Open button allows Scan Results to be viewed in the Standalone Viewer.

## 2. Review Scan Results

### Capture and Navigation Toolbar

Located vertically on the left side of the application is the capture and navigation toolbar. This toolbar will allow navigation through the results and will be visible when in Review Scan Results. The following buttons are located on this toolbar:

Option	Function
 Summary	Access the Summary view.
 Pictures	Access the Pictures view. This shows a gallery view of all pictures identified by the Captures in the Search Profile
 Videos	Access the Videos view where it is also possible to access the frame view and video player functionality
 Keywords	Access the Keywords view showing keyword hits from keyword searches
 Timeline	Access the Timeline view showing a listing of all Artifact and File Capture records in a single timeline
 Files	Access the Files View which lists all files and folders upon the target devices

Option	Function
	A log of encountered protected files and parsing or scanning events
	Access the Tagged View which lists all tagged items
	Access the Report creation view
	Access to individual Capture results

When clicking the More button, the following panel is displayed:

**More Button View**



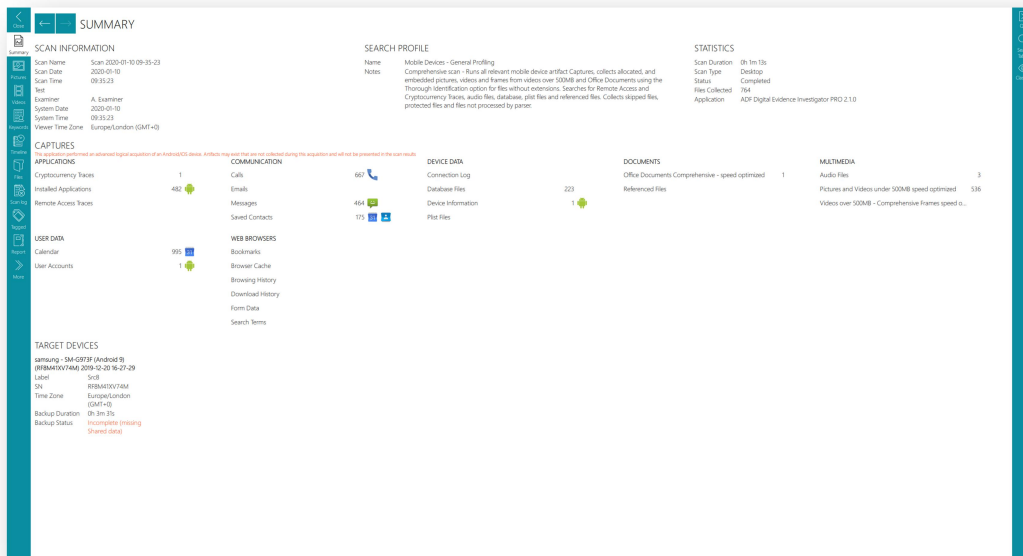
This shows at a glance all the captures and their results which are hyperlinked, clicking on a capture name will open the relevant capture.

It should be noted that captures running a keyword search within files will display the number of files identified and not the number of keyword matches identified overall.

## Summary View

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

### Summary View



The Scan Information section details the Scan Name, Scan Date and Scan Time, the System Date and System Time and the Viewer Time Zone.

The Search Profile section shows the Search Profile used to generate the Scan Results and any associated Notes on the Search Profile.

The Statistics section shows the Scan Duration, the Status, the number of Files Collected and the application and version number used. The Tags Statistics are also shown if any exist.

The Scan Status can be one of 7 outcomes as shown in the table below. Any status other than Completed is shown in red.

Scan Status	Event	Scan Log Message (in scan log)
Completed	Scan completed successfully	NA
Interrupted	User stopped the scan	Scan was paused by the user.
Crashed	Application crashed during the scan	NA
Out of Storage	No space left on destination drive during scan	Destination drive ran out of storage space.
Incomplete	Not all files can be cached	File system metadata is corrupted for source or partition. Setting scan status as Incomplete as not all files could be cached.
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 results found. Each of the Capture names are hyperlinks and by clicking them the individual Capture results are displayed.

The Target Devices section shows the details of the target devices that were scanned.

At the top left side of the screen are the Backward and Forward buttons. These allow navigation backwards and forwards between screens.







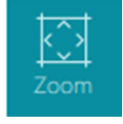


#### Backward and Forward Buttons


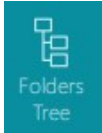





## Function Toolbars

A Function Toolbar is located vertically on the right side of the results viewer. This toolbar is context specific and will adapt depending on what is being viewed:

Function	Option
Closes the application immediately	 Quit
Opens a different set of scan results	 Open
Search the scan result tables for specific Keywords	 Search Tables
Add, remove or reorder columns from view. Changes made to column display also modify columns displayed within reports. Adjust sort order of displayed results	 Columns
Deselects (unchecks) any selected records within the current view	 Deselect All
Allows the application of context specific filters to the displayed records	 Filter
Zoom function allows for resizing of preview thumbnails	 Zoom
Apply Tags for selected record(s) in the current view. Renaming of Tags is available here.	 Tags
Apply a Comment to selected record(s) in the current view	 Comments




Function	Option
Displays Classifier progress and allows the Classifier to be paused and resumed. Facilitates access to the Pictures view, filtered by a Visual Class	 Classifier
Only visible in the Files view. Toggles the path filter displayed as a hierarchical view of folders	 Folders Tree
Toggles the display of the Details Pane which provides further information and functionality for the selected record	 Details

## Details Pane


The details pane 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 side of the details pane. The following table lists the options available in the details pane:

Option	Function
Properties	Individual properties of the selected record
Metadata	Metadata extracted from the selected file
Excerpts	Displays up to 1000 keyword hits highlighted in yellow with surrounding text visible
Frames	Displays 50 frames taken at regular intervals from a video file
Preview	Pictures are viewable in this pane at their actual size, "other files may be viewed by clicking the Undock button on the Details Pane Function Toolbar. Videos are playable via an internal player subject to installed codecs


### Function Toolbar of Details Pane

Function	Option
Undocks the Preview window	
Open the file with an external application	
Save the file to a chosen location	


### Column controls




Left click and hold in between columns will allow the resizing column widths



Drag column name up and down in the Columns function pane to reposition column L or R  
Show or hide a column by using the checkbox





Left click, hold, drag to reposition column L or R



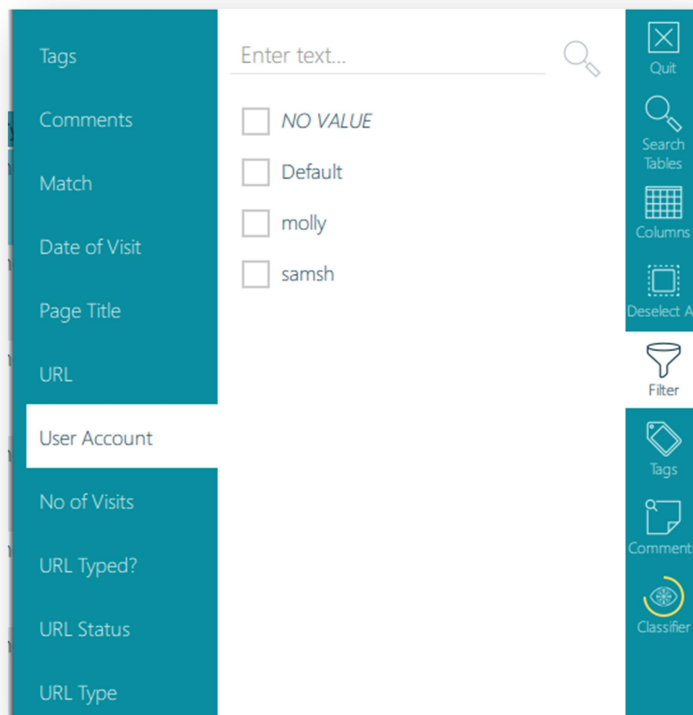
Click on the column header to sort Ascending or Descending (not all columns are sortable)

## Filtering

Filtering is achieved by selecting the Filter button on the function toolbar. This will open the filter pane and present filters for the current view. After selecting the filter click the *APPLY* button on the bottom of the Filter Pane. To remove the filter, click the  icon on the filter above the table view or click the  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.

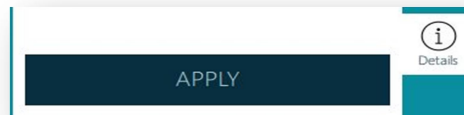
Some fields can be filtered by pre-set values or by entering text. If text is entered into the “Enter text” field the magnifying glass button within the field must be clicked.


### Filter Options



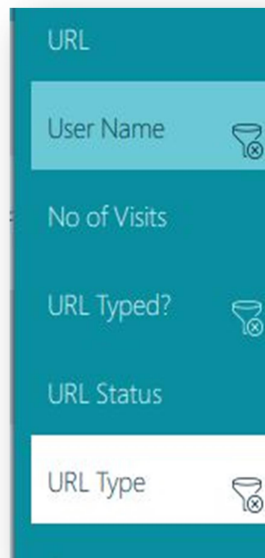
Click the Apply button to apply the filter.


### Filter Apply Button



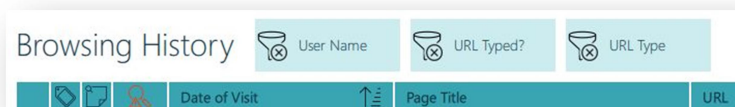
Active Filters are shown next to the column name that has been filtered (represented by the  icon). The filter can be removed by clicking on that icon.

### Active Filters



Active filters are also shown on the top of the columns with the  icon. These filters can be removed by clicking on that icon.

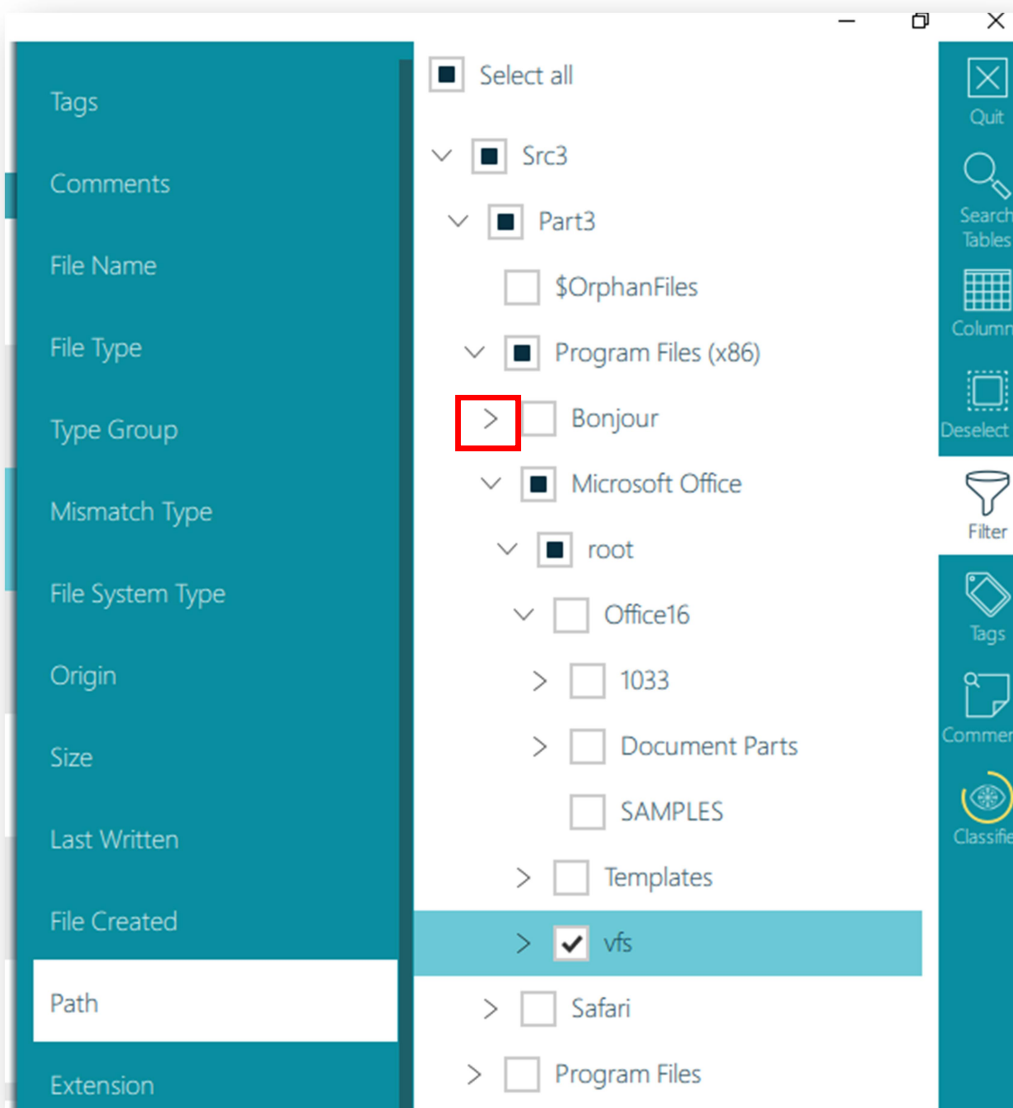
### Active Filters



## Filtering by Path

Enables the filtering of displayed files by path.

1. Clicking the Path option allows the results to be filtered by path. A selected folder indicates that all the items within that folder and any sub folders are selected. A black check box indicates a partial selection. Clicking the > icon will display sub folders.



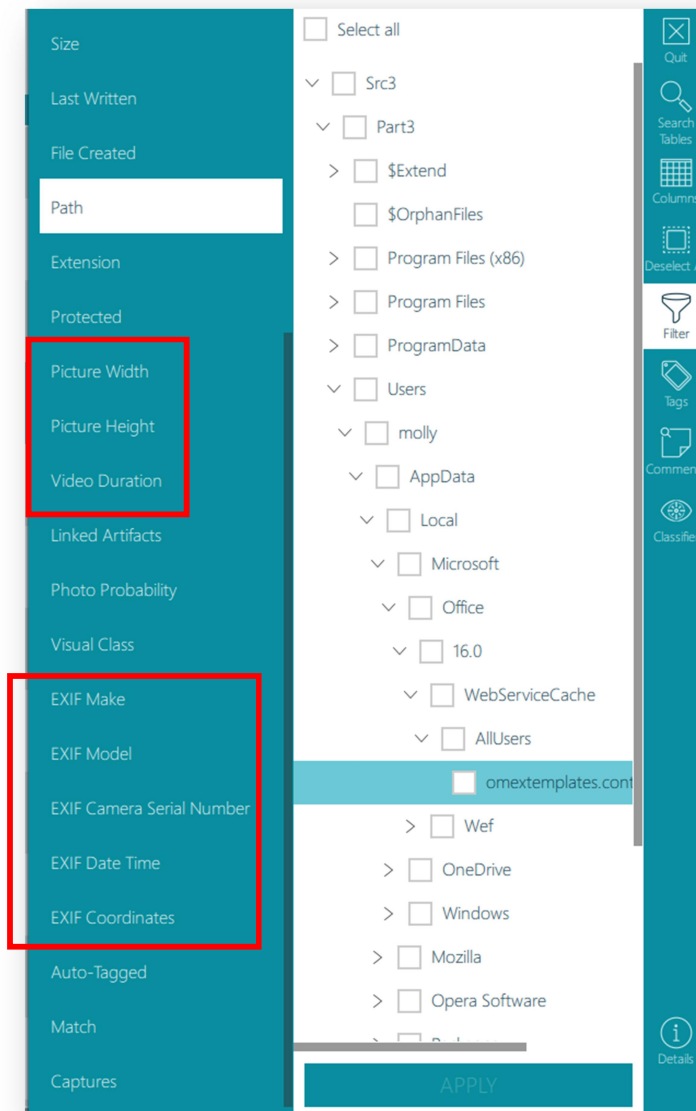


## Enhanced Filtering Pictures & Videos

Within the Pictures view or Capture view it is possible to filter within a Picture Width and Picture Height range. Within the Videos view or Capture view it is possible to filter by Video Duration (where this information has been extracted).

EXIF data such as Make, Model, Camera Serial Number, Date/Time and GPS Coordinates can also be filtered here.

### Picture and Video Filter Options



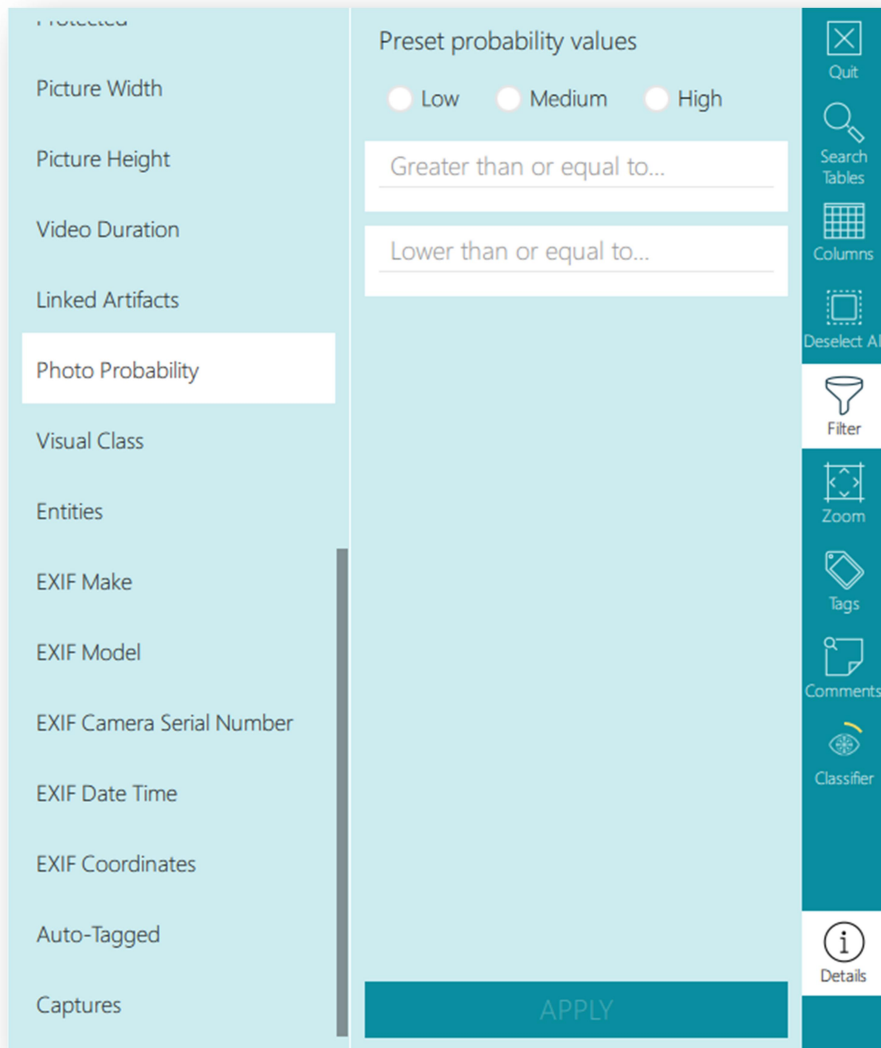


## Photo Probability

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 of 70% or more are highly likely to be a photograph as opposed to other graphic file types such as icons and clipart or similar.

The Picture and Capture views can be sorted based on the Photo Probability score, allowing non photographic graphic files 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.

### Photo Probability Filter Options

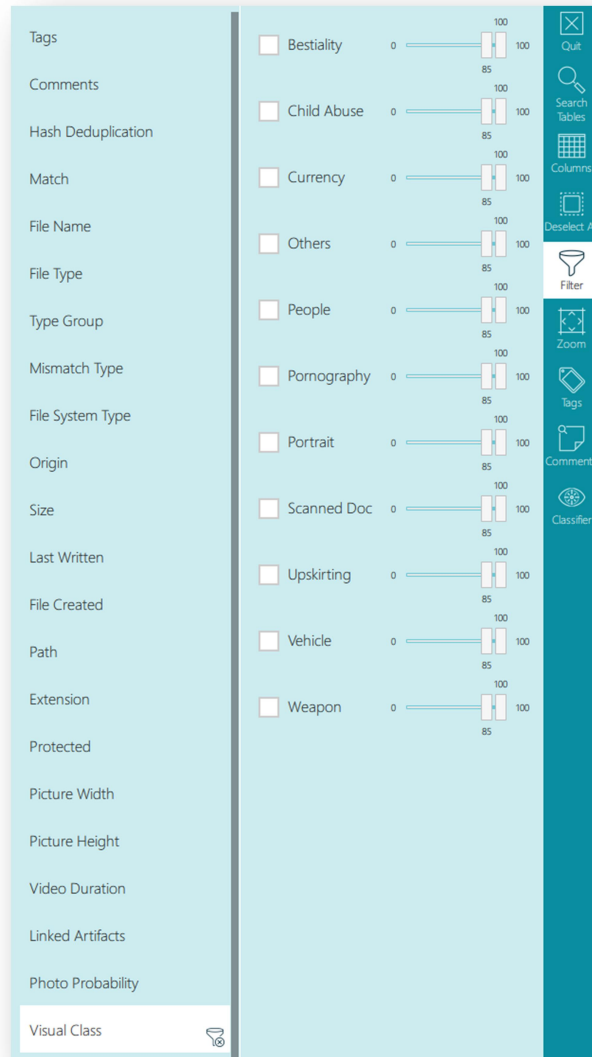


## Visual Class

If the scan results have been partially or entirely processed by the Classifier, picture file types may be filtered by one or more of 11 visual classes. The visual classes are:

Bestiality, Child Abuse, Currency, Others (various innocuous class types), People, Pornography, Portrait, Scanned Doc, Upskirting, Vehicle, Weapon.

### Visual Class Filter Options



Each picture is processed by the Classifier in order to determine how likely it is to feature within a particular class and is given a probability score. A high visual class probability score indicates that the picture concerned is more likely to fall within that visual class.

Assigning a visual class score is not an exact science and some pictures may appear to be misclassified. However if the scan results include pictures that would correctly fall within a particular class, in most tests, filtering that class to show the top 15% would result in the filter displaying pictures belonging to that class.

Visual class scores filters can be adjusted in 5% increments.

The Classifier classifies automatically in the background as soon as the scan completes. Classifier progress is shown by the Yellow line around the Classifier icon.

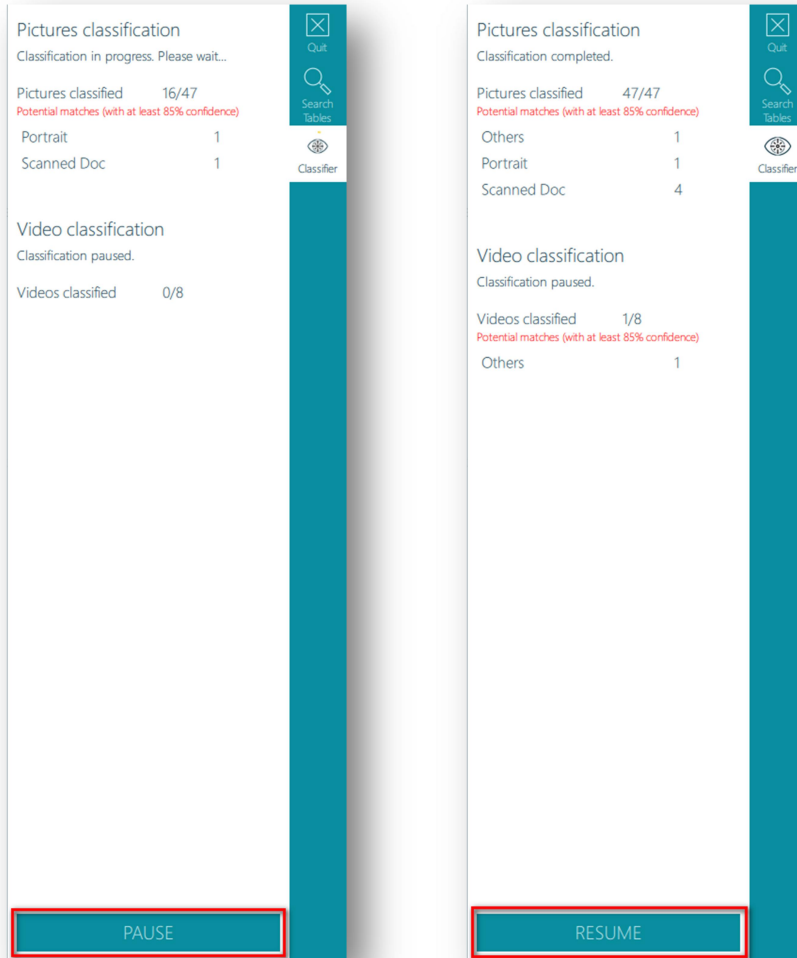
### Visual Class Filter Options



### Pausing the Classifier

The Classifier can be paused and will not start again until the Resume button is pressed.

#### Visual Class Filter Options



If the Classifier is running whilst the Scan results are closed then it will resume automatically the next time the Scan Results are opened.

## Sorting

Each table view will have different columns depending on the type of capture being viewed. A column, if sortable, will display whether ascending or descending with an arrow and line icon when clicked. Only one column can be sorted in each view.

Ascending	Descending

## Records Selection and Navigation

There are several options for selecting records to be tagged or commented:

### A Selected Picture

	Preview	File Name	File Type	Type Group
<input type="checkbox"/>				
<input checked="" type="checkbox"/>		iNode1669281	Portable Network Graphic	Picture

1. Select one record - Single click or by pressing the space bar
2. Select or Deselect multiple records:  
 Shift + Click - select first record then shift and click on last record  
 + (Plus) - Selects all fully visible records  
 - (Minus) - Deselects all fully visible records
3. Page Down - . (Period on number keypad) or Page Down key. Moves the selected view a page at a time
4. Page Up - \* (Star on number keypad) or Page Up key. Moves the selected view a page at a time

5. Navigation between records can also be achieved using:
  - Arrow keys (left -right-up-down)
  - Scroll bar
  - Mouse scroll wheel

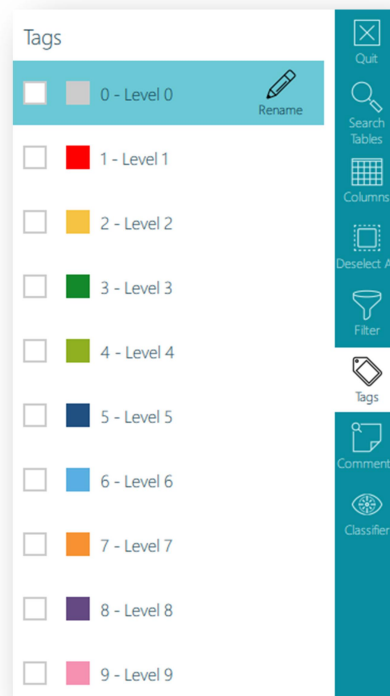
## Tagging

After selecting records there are ten (10) tags available that can be customized to suit the report. The default tags are named Level 0 through Level 9 and can be customized in the Settings view or by selecting Rename in the Tags function. Renamed Tags will be applied to the current scan results and do not apply to previous scan results.

1. To tag records with a specific tag:
  - Select record(s) then select the appropriate tag in the Tags function
  - Or select record(s) then press number key 0-9 as appropriate
  - Records can have multiple tags

To un-tag a record

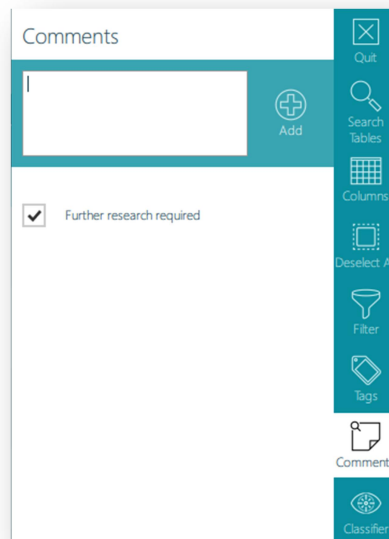
  - Select record(s) to be untagged then select the tag to be removed from the Tags function
  - Or select record(s) to be untagged then press number key of the tag to be untagged



## Comments

Comments can be added to individual or multiple selected records by clicking the comments button on the function toolbar. Clicking on the comment button opens the comment pane with a text box. Comments will be saved in a list under the Comments text box. Highlighting the individual comments will reveal an edit and delete button for that comment.

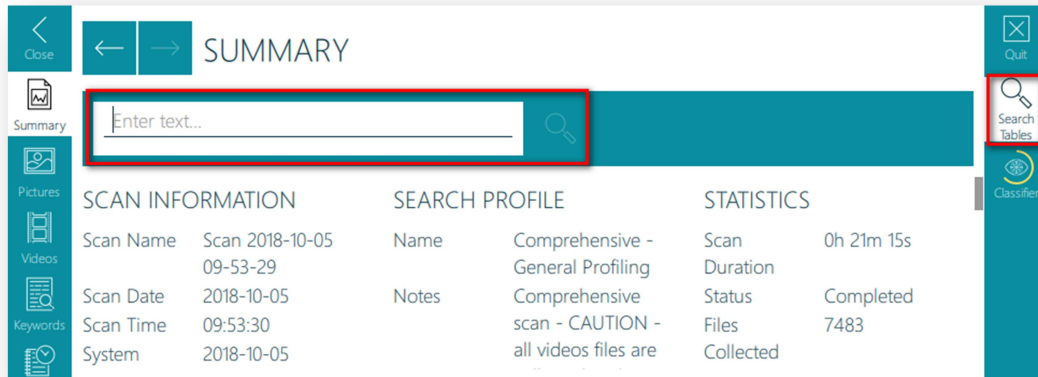
1. To add a comment to record(s):  
Type the comment in the text box and click add  
The comment will be added to the selected records
2. To remove/edit/delete a comment from record(s):  
Select records with comment(s)  
Open Comment function  
Deselect comment - Affects selected records only  
Edit Comment - Affects all records with that comment  
Delete Comment - Affects all records with that comment



## Search Scan Results

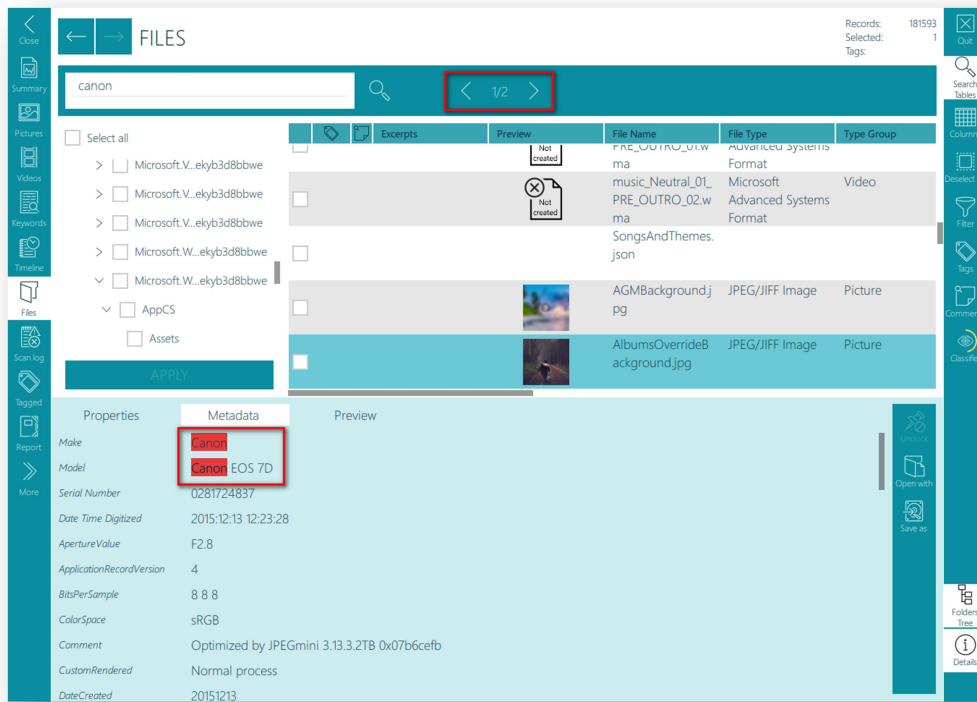
A keyword search can be carried out within the data contained in capture result tables. This keyword search is searching **only** the textual data within the results of Artifact Captures and the Files view.

1. To carry out a search click the Search Tables button. This opens up a text box for the search term, clicking the magnifying glass button alongside will carry out the search.

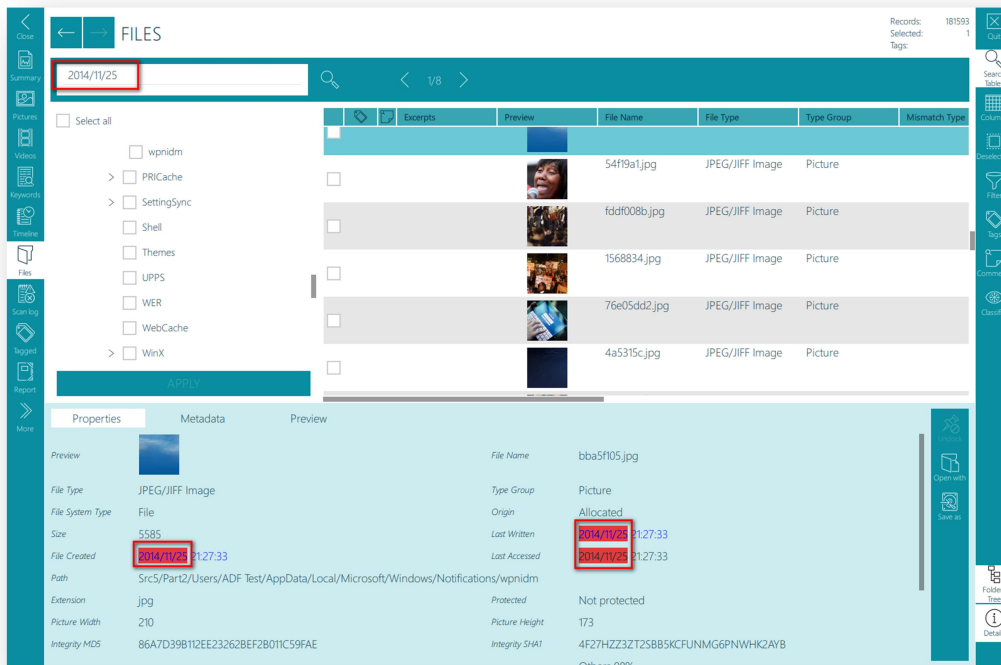


2. The search bar will identify how many search results there are and allow navigation between them using the < and > buttons. The search term will be highlighted in red. The location of search hits is indicated above the search bar.





- 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.





## Timeline

The Timeline view lists all file and artifact records that have timestamp information. The contents of the Activity, Info and Virtual Location columns are context specific and contain data relevant to the type of record displayed.

**Timeline View**



File Collection capture records list, within the File Created and Last Written columns, timestamps that hyperlink to the appropriate point within the Timeline View. Artifact Capture

records may contain timestamps. Where these timestamps exist they hyperlink to the appropriate point within the Timeline View.

Timeline records that relate to a file may contain, within the Details view of that file, a hyperlink to the Files View filtered by the path of the file concerned.

## Files

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 may also be accessible via hyperlinks from several differing artifact captures (e.g. Download History, Recent Files). File Collection 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.

### Files View



Files View records list, within the File Created and Last Written columns, timestamps that hyperlink to the appropriate point within the Timeline View. Files View records list, within the Linked Artifacts column, hyperlinks to any Artifact Captures that references the file shown.

## Messages

Artifact Captures that result in the identification of messages are displayed in the Messages view.

### Messages View

	Message Thread	Message	Attachment Name	Date/Time
<input type="checkbox"/>	7	Unread message 100220-1606 447452938009 (Martin Mulholland) - 16:06:10		2020/02/10 16:06:10
<input type="checkbox"/>	7	Snow lying now 447452938009 (Martin Mulholland) - 16:02:32	15813505528674... [Referenced Files] [Pictures and Vi...	2020/02/10 16:02:32
<input type="checkbox"/>	7	Group message from Martin 100220-1602 447452938009 (Martin Mulholland) - 16:02:03		2020/02/10 16:02:03
<input type="checkbox"/>	7	Group message from Tom 100220-1601 447493764850 (Tom) - 16:01:02		2020/02/10 16:01:02
<input type="checkbox"/>	7	Group message from James 100219-1600 447452938011 (James McLevy) - 16:00:22		2020/02/10 16:00:22
<input type="checkbox"/>	7	408072901786790658 447452938011 (James McLevy) - 15:59:39		2020/02/10 15:59:39
<input type="checkbox"/>	7	Test Viber Group 447452938011 (James McLevy) - 15:59:15		2020/02/10 15:59:15
<input type="checkbox"/>	7	Test Group 447452938011 (James McLevy) - 15:58:50		2020/02/10 15:58:50

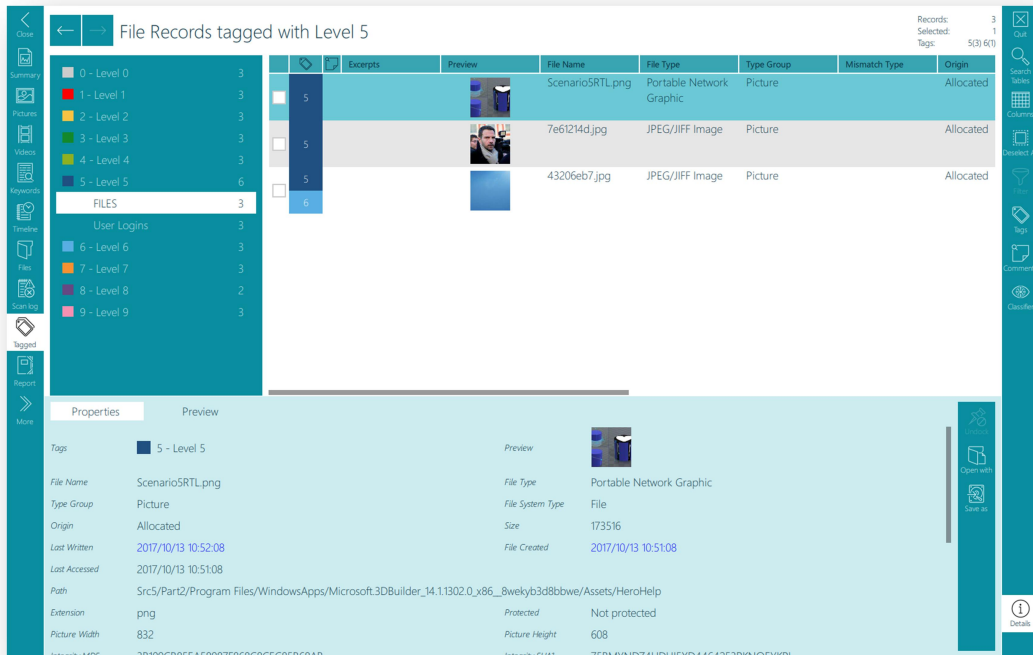
The Messages view will display the message content in the Message column. Messages sent by the local user, known as Outgoing messages, will be displayed in a blue message bubble that is right aligned in the Message column. Messages sent from others to the local user, known as Incoming messages, will 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. It is not possible to determine a message thread for all message applications.

## Tagged View

The Tagged view lists all tagged records.

### Tagged View



All tagged records are accessible from this view. Each tag where appropriate will indicate the Artifact and File records associated with it.

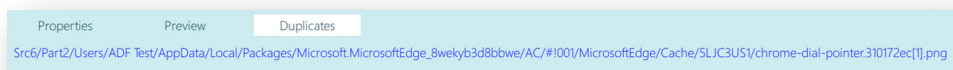
## Duplicate Files

Files with matching hash values and file size identified during a scan are considered duplicate files. It is possible to identify duplicates of a file within the Files view and the Pictures view will display an icon to show a picture has duplicates.

### Files View

Within the Files view, duplicate files are displayed in the details pane. Duplicate files are shown as a hyperlink which, when clicked, will display details for the duplicate file.

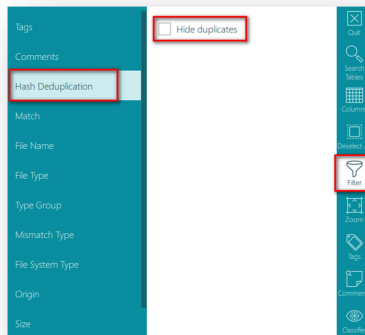
#### Duplicate Files in Details Pane



### Pictures View

The Duplicates tab appears within the Pictures view. A Hash Deduplication option is also available within the Filter options. Selecting the Hide duplicates option will only display one picture in the gallery view if duplicates of the picture are identified.

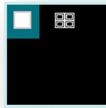
#### Hash Deduplication Filter



Pictures that have duplicates will display an icon showing that duplicate pictures were identified:

#### Duplicate Picture Icon





## Referenced File Functionality

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). We refer to these files as Referenced Files.

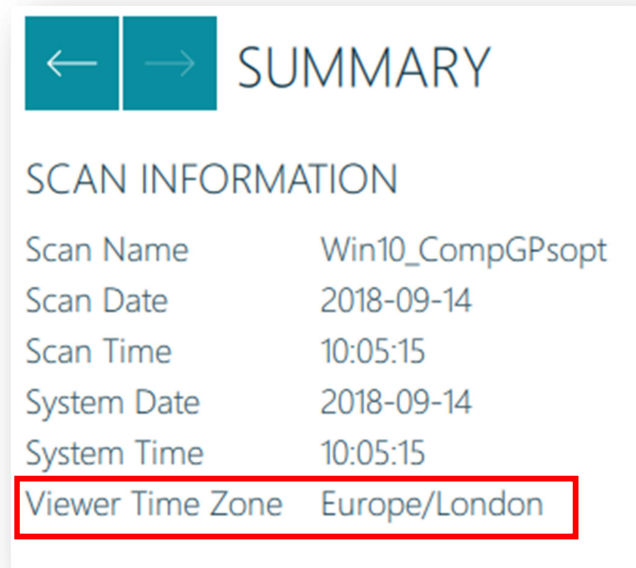
Artifact Capture	Notes
Recent Files	This Artifact Capture identifies recently accessed files. Recently accessed files that can be located upon the target device(s) are treated as Referenced Files and are accessible by a hyperlink in the Candidate column to the relevant file record in the Files View. 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 Collections 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 Collection Captures that have collected the file concerned.

Artifact Capture	Notes
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 Collection 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 Collection Captures that have collected the file concerned. The Attachment Names column can also contain details of other Captures that reference the file.

File Collection capture records list, within the Linked Artifacts column, hyperlinks to any Artifact Captures that references the file shown.

## Time Zone Section

### Viewer Time Zone in Summary View



When scans are carried out upon system drives the scanner tries to establish the configured time zone. If a time zone is established all timestamps that are displayed within the results viewer are adjusted where necessary to reflect the configured time zone. Within the Summary view the Viewer Time Zone value will reflect the established time zone.

When scans are carried out on multiple target devices in one scan the scanner searches for a system drive and if one is found establishes the configured time zone. If a time zone is established all timestamps that are displayed within the results viewer for all target devices are adjusted where necessary to reflect the configured time zone. If multiple system drives are located the most recently used system drive takes precedence and all timestamps that are displayed within the results viewer are adjusted in accordance with the time zone discovered on this device. In these cases, within the Summary view the Viewer Time Zone value will reflect the established time zone.

When scans are carried out upon target devices that are non-system drives (without an operating system) no timestamp adjustment is carried out. In this case within the Summary view the Viewer Time Zone will reflect the time zone used by the viewing computer.

In cases where the scanner cannot establish the time zone on system drives no timestamp adjustment is carried out. In this case within the Summary view the Viewer Time Zone will reflect the time zone used by the viewing computer.

## Reviewing Screenshots

Scans of mobile devices can include screenshots taken from the device. Clicking on Screenshots within the Summary screen will load the Screenshots view.

### Screenshots View

The screenshot shows the 'Screenshots View' interface. At the top, there's a navigation bar with a back arrow, a forward arrow, and the title 'Screenshots'. On the right side of the navigation bar, it shows 'Records: 1', 'Selected: 1', and 'Tags: 1'. Below the navigation bar is a list of applications with their respective screenshot counts:

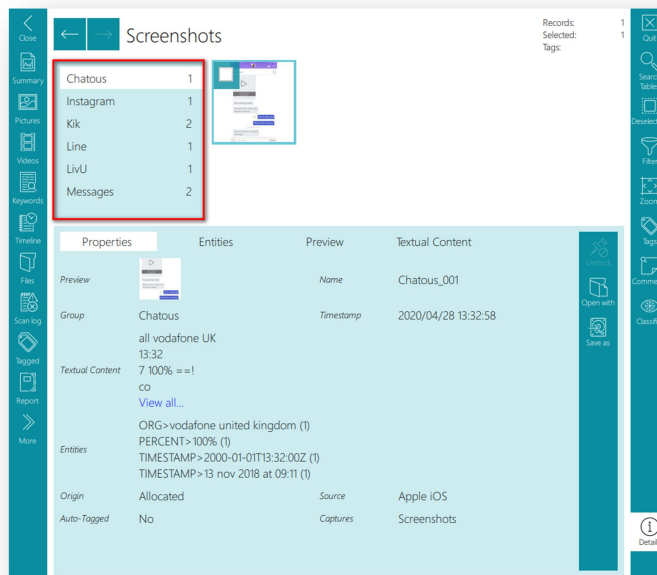
- Chatous: 1
- Instagram: 1
- Kik: 2
- Line: 1
- LivU: 1
- Messages: 2

A small thumbnail of an Instagram screenshot is shown next to the Instagram entry. Below this list is a detailed view of the selected screenshot, which is an Instagram post. The detailed view is organized into four columns: Properties, Entities, Preview, and Textual Content.

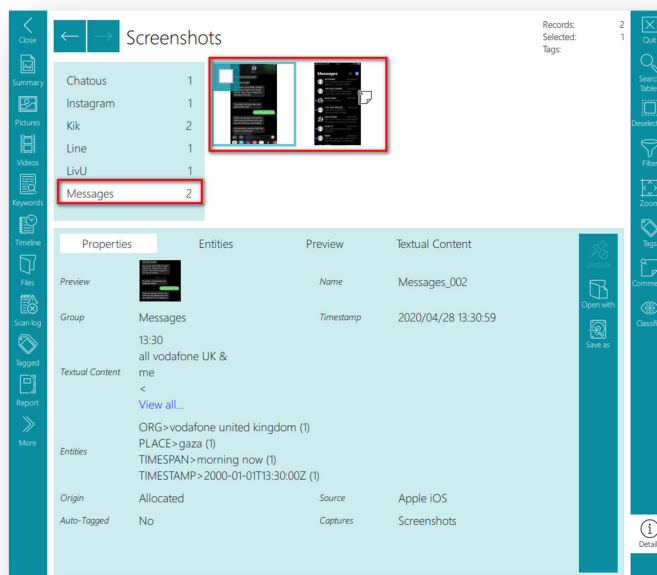
Properties	Entities	Preview	Textual Content
Preview		Name	Instagram_001
Group	Instagram	Timestamp	2020/04/28 13:34:41
Textual Content	e oda Oo V <a href="#">View all...</a>	Entities	PLACE> aa (1) PLACE> ny (1)
Origin	Allocated	Source	Apple iOS
Auto-Tagged	No	Captures	Screenshots

On the left side of the interface, there is a vertical navigation menu with icons for: Close, Summary, Pictures, Videos, Keywords, Timeline, Files, Scan log, Tagged, Report, and More. On the right side, there is another vertical menu with icons for: Quit, Search Tables, Deselect All, Filter, Zoom, Tags, Comments, Classifier, and Details.

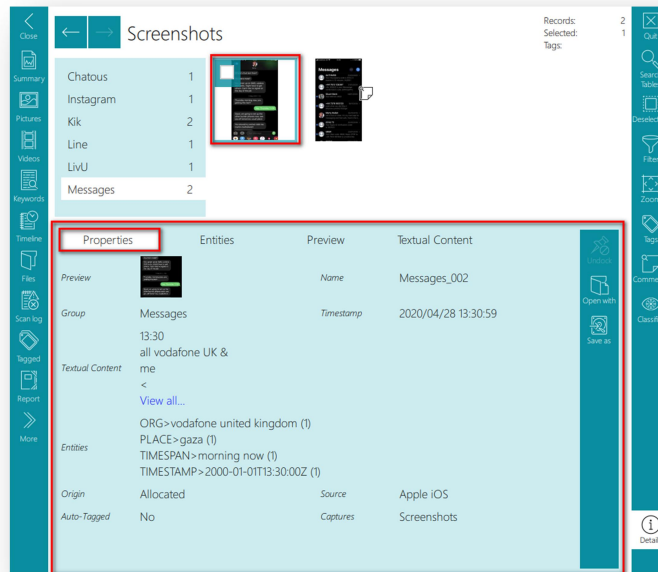
1. The left hand pane shows the Screenshot Group names entered when the screenshots were taken



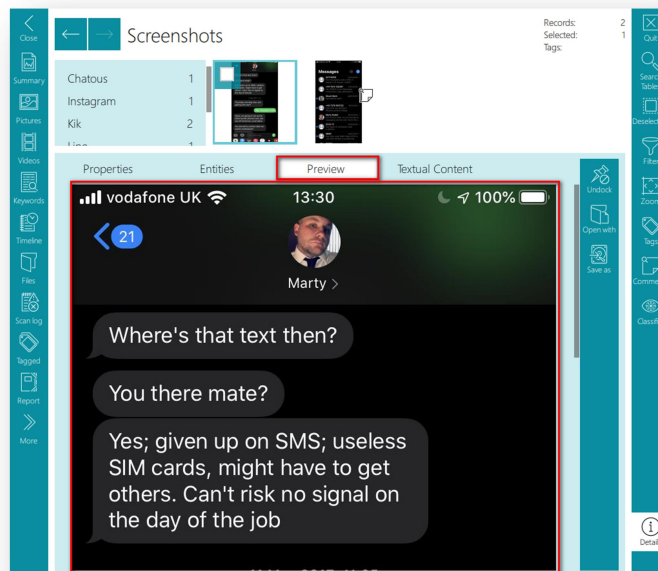
2. Clicking on a Screenshot Group name will show a gallery of screenshots taken under that name



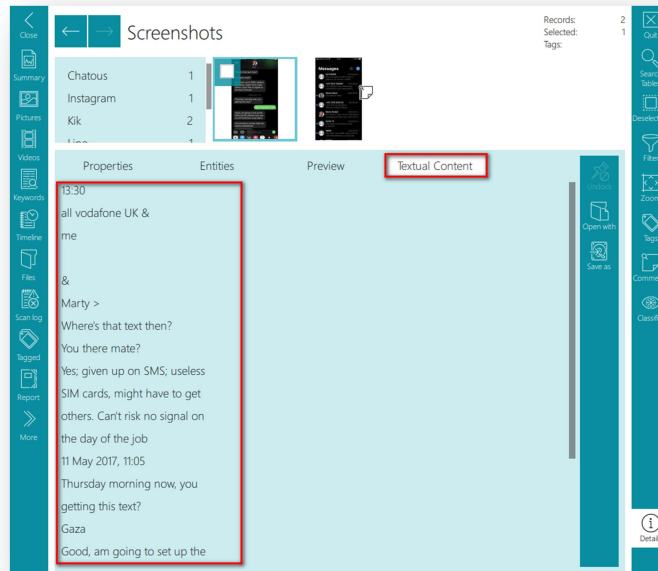
3. Clicking on a screenshot in the gallery will update the Details pane. The Properties tab will show details associated with the screenshot such as the name, the date/time the screenshot was taken and any user entered comments



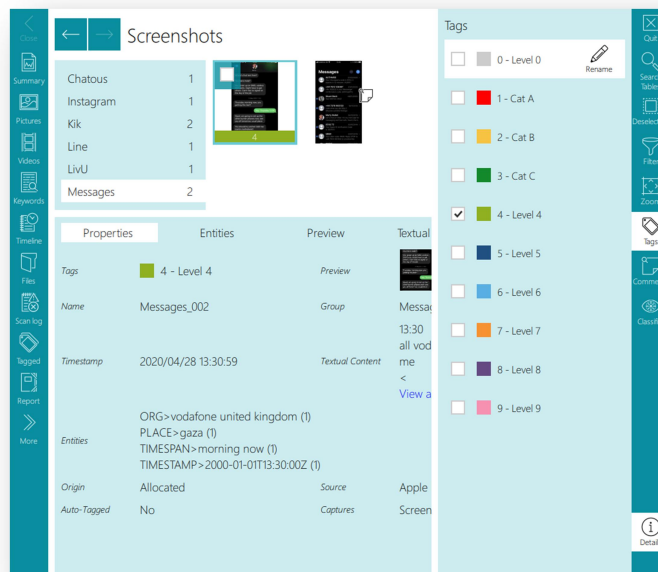
4. The Preview tab will show a full size image of the screenshot



5. The Textual Content tab will show any text information that was extracted from the screenshot. The textual content may not accurately reflect the text that was present on screen at the time and some text may not have been identified. 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



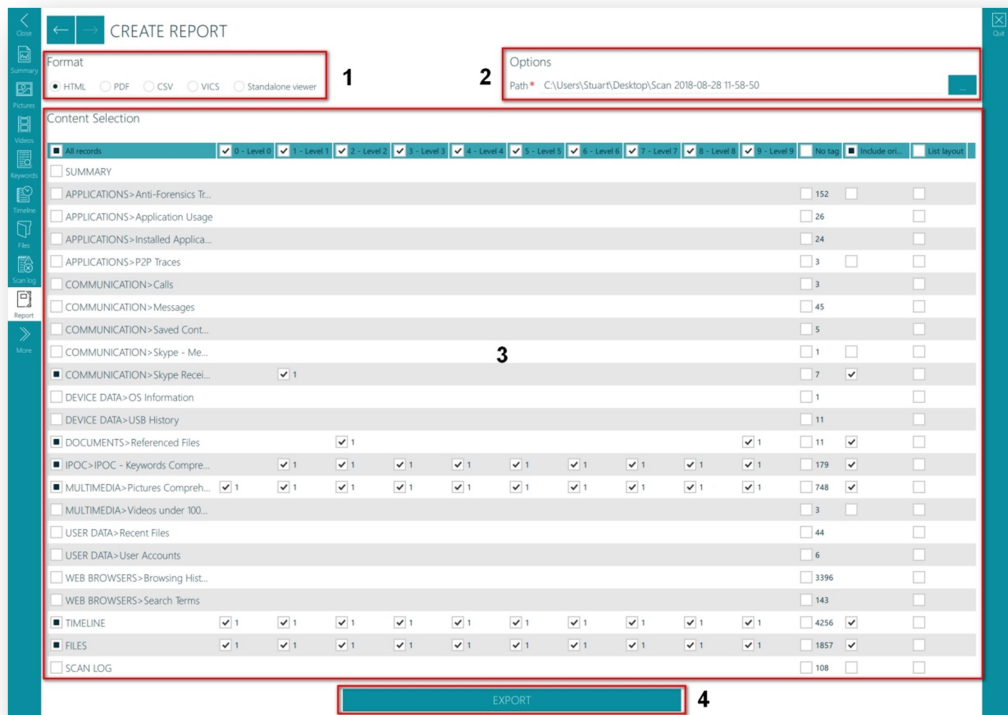
6. Screenshots can be tagged like any file or record



### 3. Reporting

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.

#### Report View



The Create Report view has 4 main sections:

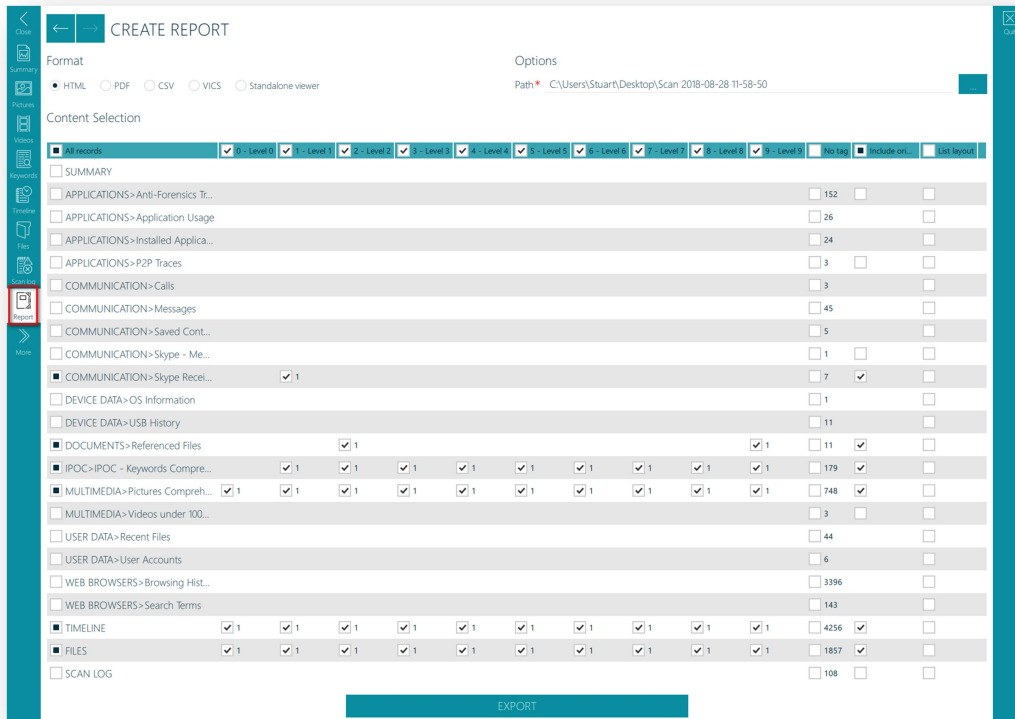
Section	Functionality
1 - Format	Select the desired report output
2 - Options	Choose the desired output location for the report and define orientation for PDF reports
3 - Content Selection	Select the records/files desired within the report
4 - Export Button	Create the report



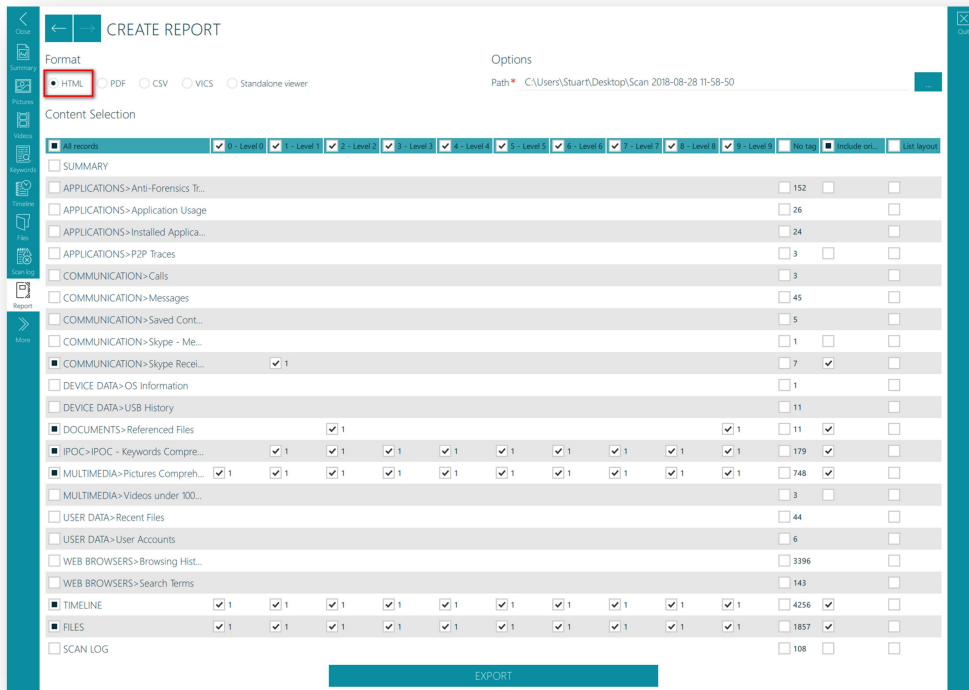
## HTML Report

HTML reports are viewable with a web browser. The HTML report is customizable allowing the choice of specific Captures and tagged items to show in the report, alternatively, all records can also be included in a report. The underlying original files may also be exported (if collected) with the report and can be opened directly from the HTML report providing there are associated applications on the computer used to view the report.

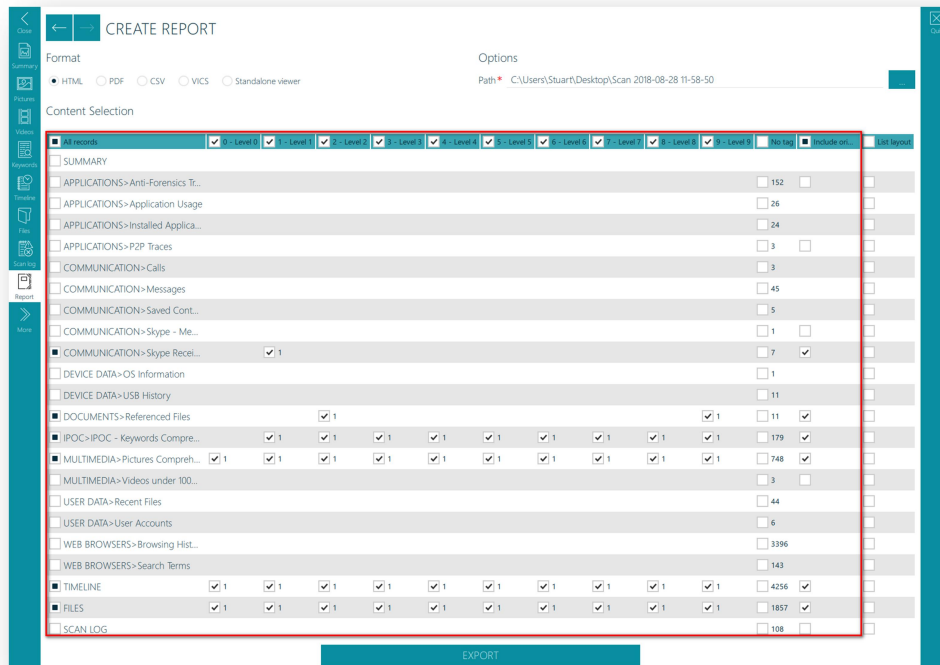
1. Click Report button.



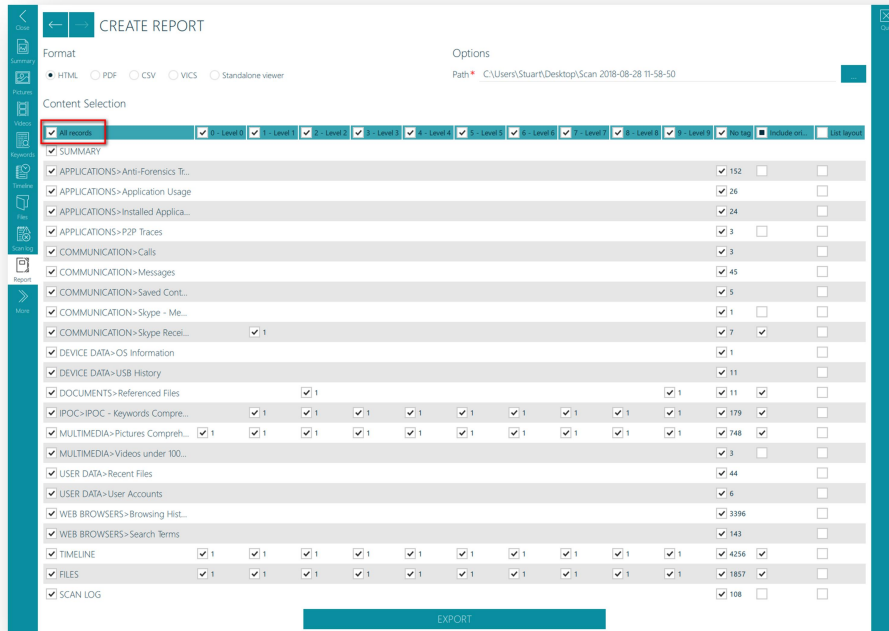
2. Select Format – HTML from the format section.



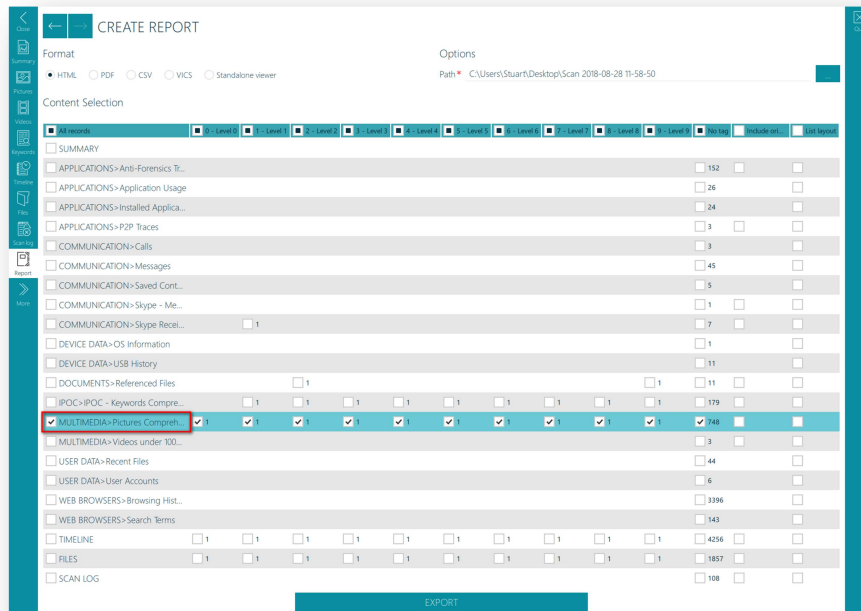
3. By default, all tagged records are selected in the Content Selection section.



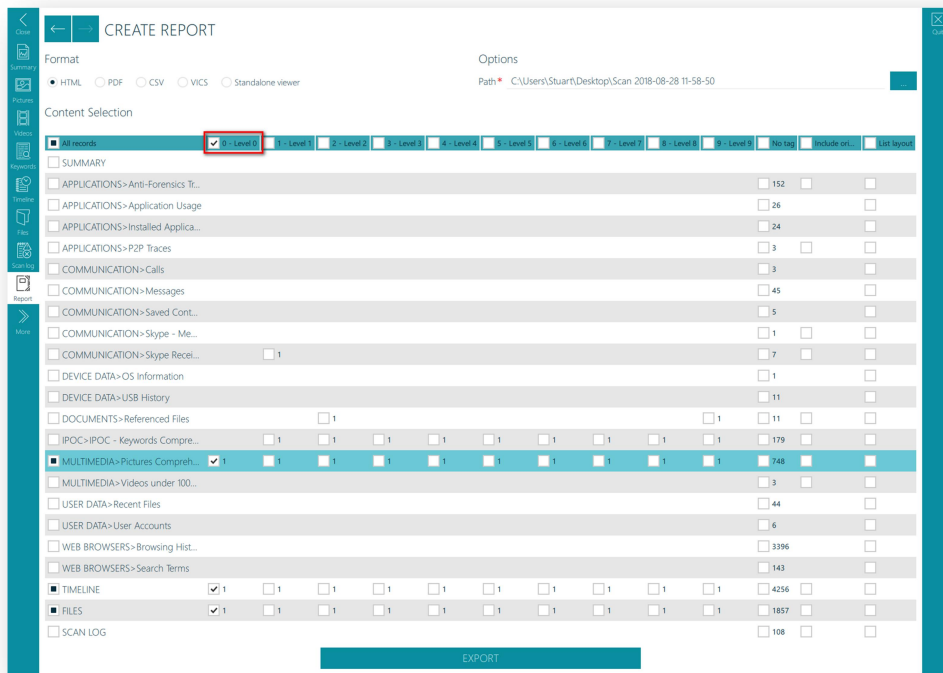
4. Optional - Select the all records checkbox to include all records.



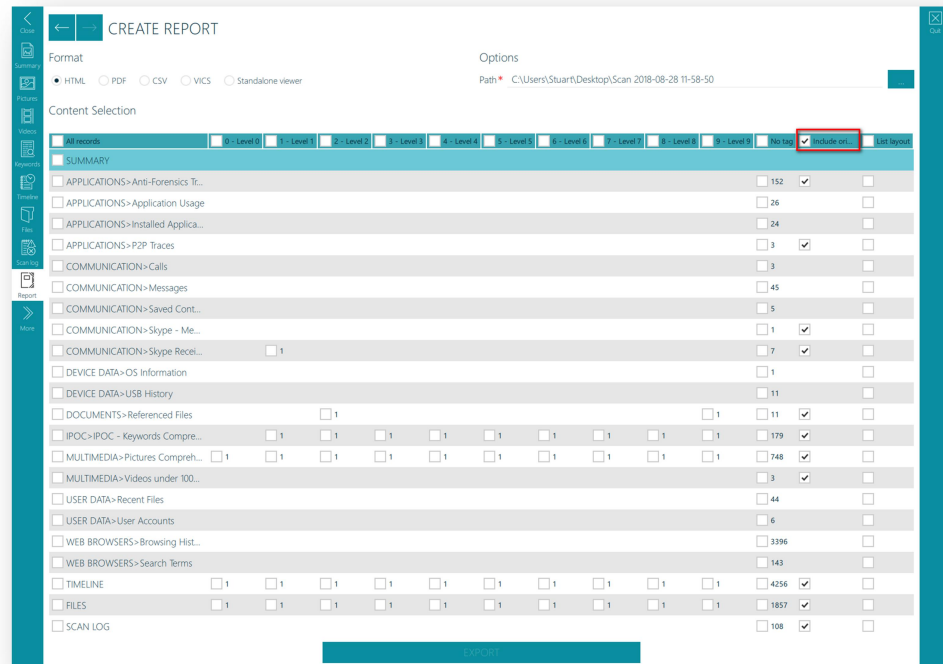
5. Optional - Select the checkbox next to each capture to include all records in that capture within the report.



- Optional - Select the checkbox above each tag column to include all of these tagged records within the report.

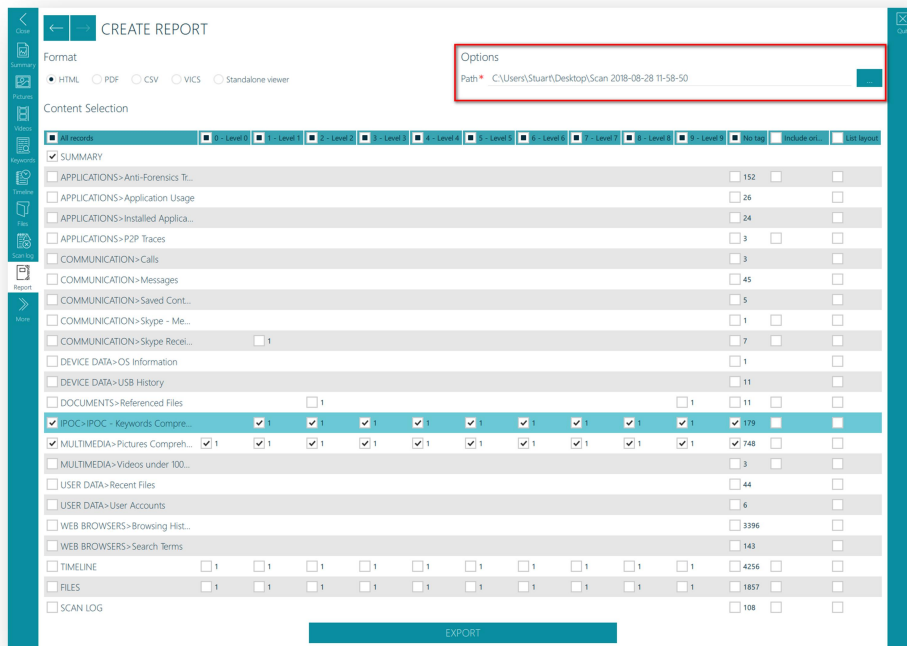


- Optional - Select the checkbox to export original files where collected.

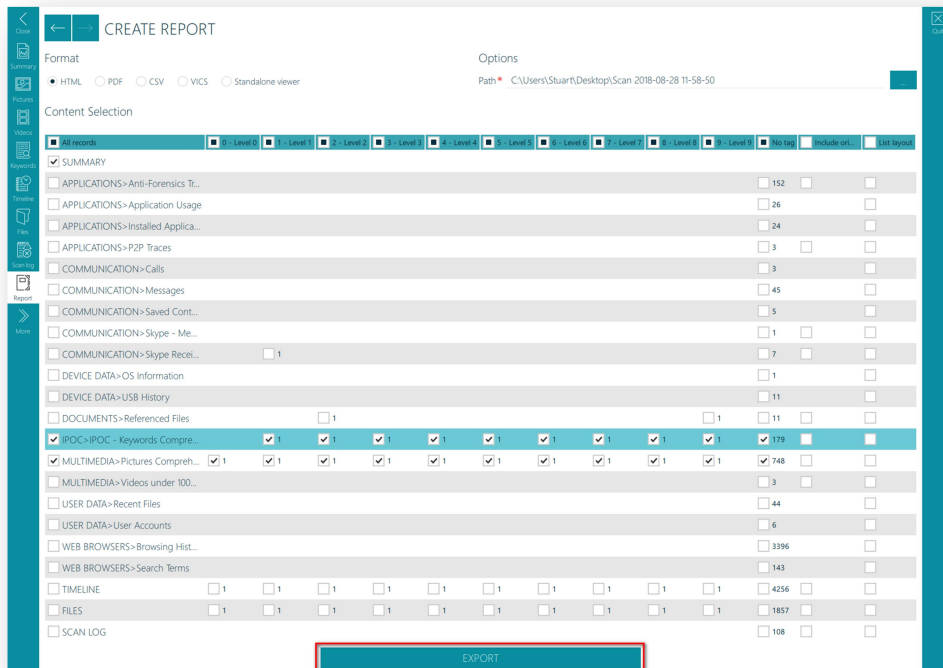




10. Optional - Choose path to save report to (default value is the Desktop of the currently logged in user, the default location can be changed in the Settings view).



11. Click on the Export button to create the HTML report.

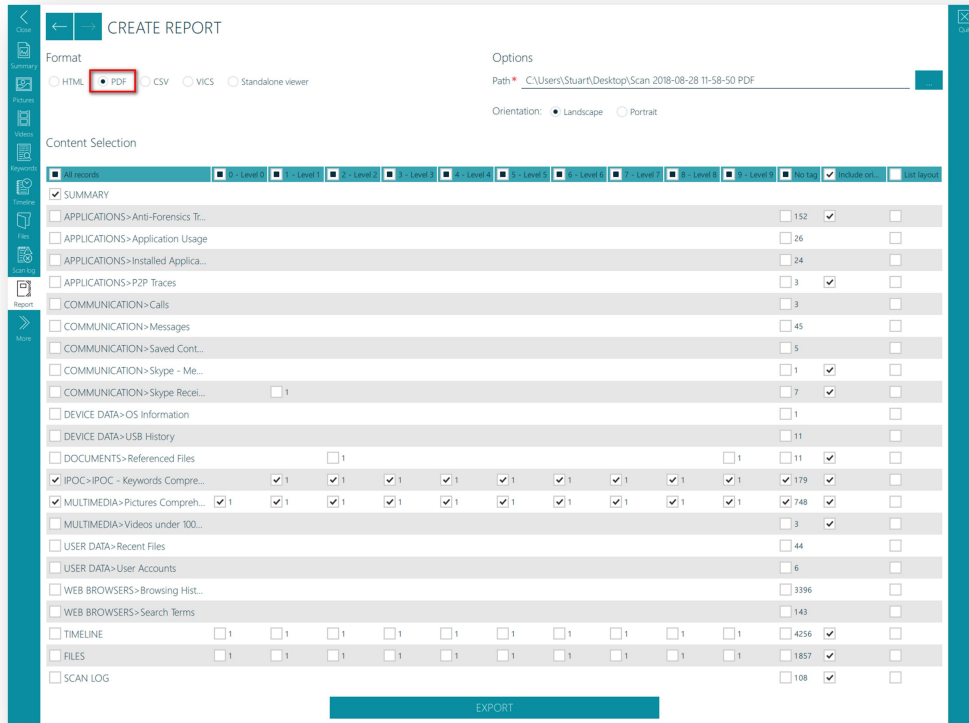




## PDF Report

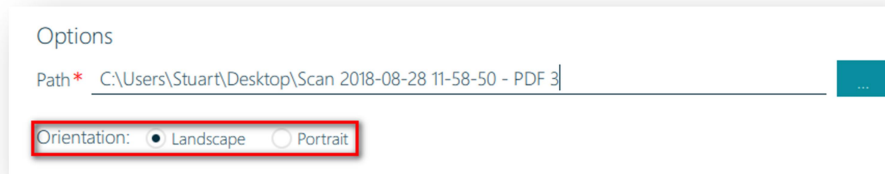
The PDF report is customizable allowing the choice of specific Captures and tags to show in the report, all records can also be shown in the report. Where files have been collected with a scan these can be exported with the report, these can then be opened directly from the PDF report providing there are associated applications on the computer viewing the report.

### PDF Report



When creating a PDF report Landscape or Portrait orientation can be selected. Reports containing a large number of columns are best produced in Landscape as some columns may not be displayed in Portrait orientation due to the limited page space available.

### PDF Orientation

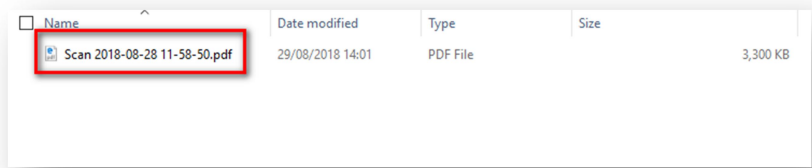




## Opening PDF Report

PDF reports are stored within a folder as specified within the Option path field. To open a PDF report, browse to the location where the folder was created, open the folder and double click on the <scan name>.pdf file therein:

### Opening PDF Report



When viewing a PDF report it will open within the default application used to open PDF files.

The PDF report displays the same columns that were visible in the viewer in the order they were displayed. To remove columns from the PDF report hide them within the viewer prior to creating the report. With limited page space it is recommended to remove columns irrelevant to the report prior to creating a PDF report.

### PDF Report

Scan 2018-08-28 11-58-50

**SUMMARY**

**SCAN INFORMATION**

Scan Name	Scan 2018-08-28 11-58-50
Scan Date	2018-08-28
Scan Time	11:58:51
System Date	2018-08-28
System Time	11:58:51
Viewer Time	
Zone	Europe/London

**STATISTICS**

Scan Duration	0h 0m 29s
Status	Completed
Files Collected	805
Application	ADF Digital Evidence Investigator 0.0.0

**SEARCH PROFILE**

Name	Comprehensive - IPOC speed optimized
Notes	Comprehensive scan - Runs all artifact Captures, collects allocated, embedded, and deleted pictures and videos, searches for common IPOC keywords, and searches for known hash values using the Thorough Identification for Files Without Extension option. Searches for anti-forensics traces, remote access traces, P2P traces and files from Skype caches. Collects protected files and files not processed by parser

**TAGS STATISTICS**

0 - Level 0	1
1 - Level 1	1
2 - Level 2	1
3 - Level 3	1
4 - Level 4	1
5 - Level 5	1
6 - Level 6	1
7 - Level 7	1
8 - Level 8	1
9 - Level 9	1

**CAPTURES**

Anti-Forensics Traces	201
Application Usage	26
Installed Applications	24
P2P Files Shared or Downloaded	0
P2P Search Terms	0
P2P Traces	3
Remote Access Traces	0
Shareaza GUIDs	0

**COMMUNICATION**

Calls	3
Emails	0
Messages	45
Saved Contacts	5
Skype - Media_cache Folder	1
Skype Received Files	8

**DOCUMENTS**

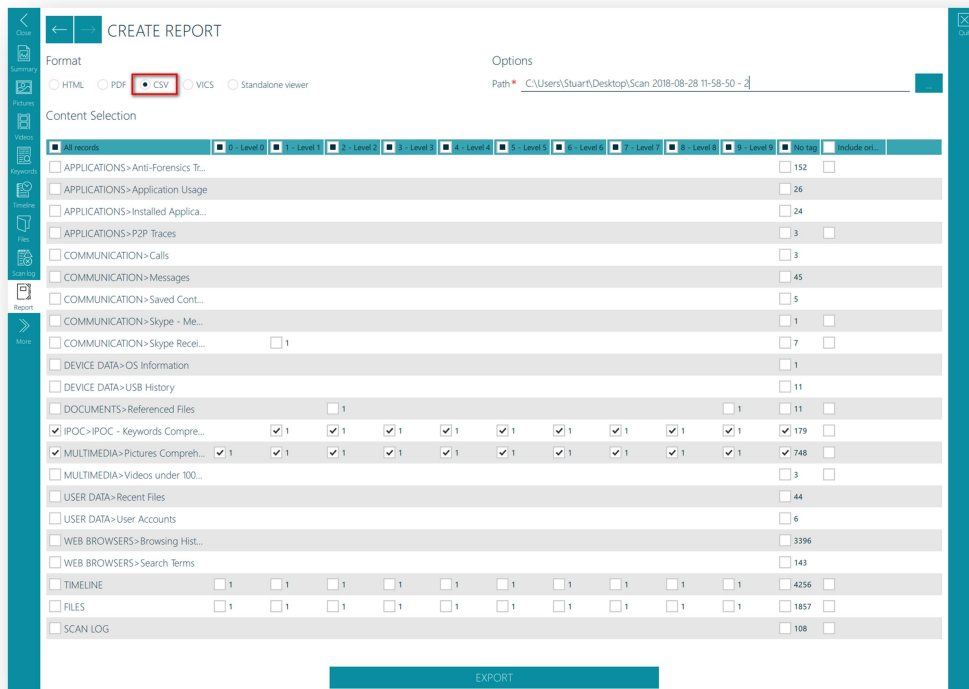
Referenced Files	13
------------------	----

SUMMARY 1 / 199

## CSV Report

The CSV report is customizable allowing the choice of specific Captures and tags to show in a report, all records can also be shown in the report. Results where files were captured can be set to export the files which will be maintained in a ZIP archive in its' original path. The CSV report has the same options as the HTML report with the exception that all the records' properties are always exported, and exporting the results in a list view is not an option. An individual CSV file is created for every capture that an item has been selected for inclusion in the report.

### CSV Report



## Opening CSV Report

CSV reports are stored within a folder as specified within the Option path field. To open a CSV report, browse to the location where the folder was created, open the folder and double click on the desired <capture>.csv file therein:

### Opening CSV Report

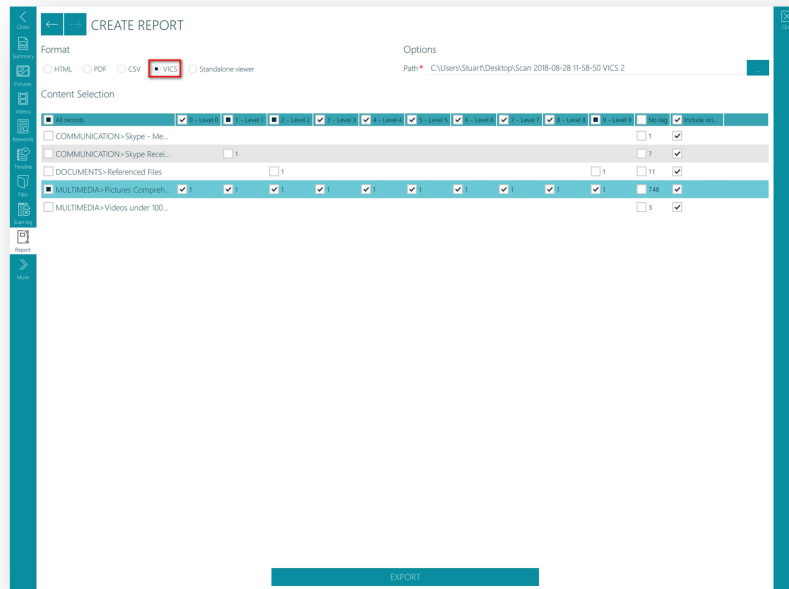
Name	Date modified	Type	Size
original_files		File folder	
APPLICATIONS-Anti-Forensics Traces-FILES.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	6 KB
APPLICATIONS-Application Usage.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	21 KB
APPLICATIONS-Cloud Storage Traces-FILES.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	30 KB
APPLICATIONS-Installed Applications.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	3 KB
APPLICATIONS-Social Media Traces-Browser Cache.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	12 KB
APPLICATIONS-Social Media Traces-Browsing History.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	16 KB
APPLICATIONS-Social Media Traces-FILES.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	8 KB
DEVICE DATA-Connection Log.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	3 KB
DEVICE DATA-OS Information.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	2 KB
DEVICE DATA-USB History.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	4 KB
DEVICE DATA-Windows Registry Files.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	8 KB
DOCUMENTS-Office Documents Comprehensive thorough ID .csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	13 KB
DOCUMENTS-Referenced Files.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	627 KB
FILES.csv	20/09/2018 10:27	Microsoft Excel Comma Separated ...	62,939 KB
MULTIMEDIA-Pictures Comprehensive Thorough ID no carving.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	3,348 KB
MULTIMEDIA-Videos All - Comprehensive Thorough ID.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	215 KB
SCAN LOG.csv	20/09/2018 10:27	Microsoft Excel Comma Separated ...	91 KB
TIMELINE.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	4,596 KB
USER DATA-Desktop shortcut files.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	2 KB
USER DATA-Recent Files.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	46 KB
USER DATA-User Accounts.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	3 KB
USER DATA-User Logins.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	199 KB
WEB BROWSERS-Browser Cache.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	965 KB
WEB BROWSERS-Browsing History.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	302 KB
WEB BROWSERS-Download History.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	4 KB
WEB BROWSERS-Form Data.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	2 KB
WEB BROWSERS-Search Terms.csv	20/09/2018 10:26	Microsoft Excel Comma Separated ...	5 KB

When viewing a CSV report it will open within the default application used to open CSV files.

## VICS Report

The VICS report option allows the creation of a Project VICS compatible output folder. This folder contains selected picture and video files together with a Project VICS compatible JSON file. This report is compatible with and can be imported into other applications that support Project VICS including Griffeye. The output Project VICS JSON file can also be used to create hash captures for use in other cases.

### VICS Report



### Using VICS Report Output

The Project VICS output is stored within a folder as specified within the Option path field. When asked to import a Project VICS JSON file within another application, browse to this location and select the *<scan name>.json* file:

### Project VICS JSON File

