

Standalone Report User Guide



Digital Evidence Investigator version 2.2



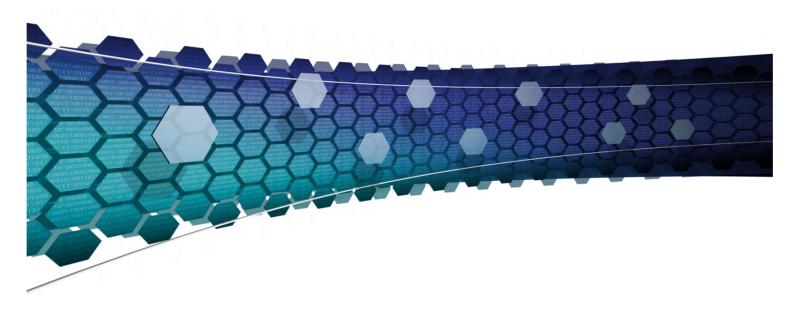
Triage Investigator version 5.2



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	
	FUNCTION TOOLBAR OF DETAILS PANE	11
	COLUMN CONTROLS	11
	FILTERING	12
	PHOTO PROBABILITY	17
	VISUAL CLASS	
	Sorting	21
	RECORDS SELECTION AND NAVIGATION	21
	TAGGING	22
	COMMENTS	23
	SEARCH SCAN RESULTS	24
	TIMELINE	27
	FILES	
	Messages	
	TAGGED VIEW	
	DUPLICATE FILES	
	REFERENCED FILE FUNCTIONALITY	
	TIME ZONE SECTION	
	REVIEWING SCREENSHOTS	
3.	REPORTING	40
	HTML REPORT	41
	PDF REPORT	
	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:

Name	Date modified	Туре	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	Scan 202	20-01-09 14-51-45					1
Scan 2020-01-09 14-51-45 Exactly Politie Mobile Devices - General Profiling Hypert Very	SCAN INFO Scan Name Scan Time System Date System Time Viewer Time Zone	RMATION San 2020-01-09 14-51-45 2020-01-09 14:51:45 2020-01-09 14:51:45 Europe/London (GMT+0)	SEARCH Name Notes	I PROFILE Mobile Decises - General Mobile Decises - General relevant mobile device antibet captures: collect and and and fames from wholes: over 5000k and Cliffle Documents beenfaction opcomment detentization opcomment of memory Ances, audo Cryptocumenty Taxes, audo Cryptocumenty Taxes, audo Cryptocumenty Taxes, audo Cryptocumenty Taxes, audo Bie, database, pite file and Bie, database, pite file and Bie, database, pite file and Bies, protected Bies and Bien not processed by paies.	STATISTICS Scan Duration Scan Type Status Files Collected Application	Ot On 275 Destop Gradeet MP Mole Device Investigator 2.10	
	APPLICATIONS Cryptocurrency Installed Applica	Traces	ndroid/OS davice. A 1 262 🌳	rtfacts may exist that are not collected during this a COMMUNICATION Calls Emails	21 V		
	Remote Access			Messages Saved Contacts DOCUMENTS	8 🖪		
	Connection Log Database Files Device Informati Plist Files		59 1 🌩	Office Documents Comp Referenced Files	rrenensive - speed op	2	
	MULTIMEDIA Audio Files	eos under 500MB speed optimize	14 d 1547	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
Scan log	A log of encountered protected files and parsing or scanning events
Tagged	Access the Tagged View which lists all tagged items
Report	Access the Report creation view
More	Access to individual Capture results



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

APPLICATIONS		COMMUNICATION		DEVICE DATA	
Anti-Forensics Traces			3 <mark>S</mark>	Connection Log	
Application Usage			17 0 7	Device Information	
Cloud Storage Traces		Messages	40 S	OS Information	
Installed Applications		Saved Contacts	16 <mark>0</mark> 7 S	USB History	
		Skype - Media_cache Folder		Windows Registry Files	
Social Media Traces		Skype Received Files			
DOCUMENTS		MULTIMEDIA			
Office Documents Compre		Pictures Comprehensive - sp			
		Videos over 100MB - Compr		Desktop shortcut files	
		Videos under 100MB - Comp			
Browser Cache	3941 🚺 😂				
	1148 🚺				

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.

CAN INFORMATION Son Name Son 2020 (1-0 0+3)- Son Tame Son			Notes	ROFILE Mobile Devices - General Profiling Comprehensive scan - Runs all relevant mod methodedid protunes, where and have from theorem and the scan of the distance produced like and file not processed by pa	videos over S00MB and Office Do out extensions. Searches for Remo plist files and referenced files. Col	cuments using the te Access and	STATISTICS Scan Dourson Oh Im 18s Scan Type Desktop Stauz Files Collected Prilo Collected Application ADP Digital Evidence Inve	regular PRO 2.10	Do Of State
CAPTURES The operation provide the adversed topical equations APPLCATONS Constructionery States Installed Applications Remote Access Traces USER DATA Calendar User Accesses	f an Android (CC device, Art 1 482 🏟 925 👥 1 🙀	ben ing works as not induced party in wighted COMMERCION Cafe Emails Served Contacts Served Contacts Biodemarks Brower Cafe Brower Cafe Brower Cafe Brower Cafe Brower Cafe Brower Cafe Brower Cafe	en and well not be prevented in the scane 667 📞 464 🥶 775 🐨 🛋	DEVICE DATA Connection Log Database Fires Device Information Pitcl Files	223 1 🌩	DOCLMENTS Office Documents Cor Referenced Files	npenhanake - speed optimized 1	NATIMIDA Andre Tin Pictures and Vibeos under SIXMB speed optimized Vibeos ow SIXXB - Comprehensive Former speed o	3 536
TARGET DEVICES smung-1MORTH Andres 9 (IMMANY AVA 200-3-20 8-7-20 (IMMANY AVA 200-3-20 (IMMANY		Samh lums							

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	terrupted 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.

E	Backward and Forward Buttons	
	$\leftarrow \rightarrow$	



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.	Res 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	(i) 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	Undock
Open the file with an external application	Open with
Save the file to a chosen location	Save as

Column controls

Q Timestamp	↓	+ Principal	Recipient
Left click an	d hold in between colum	ns will allow the resizing colun	nn widths
	 Comments Match Activity 	Columns Move Deselect All	
Drag column name		mns function pane to reposition by using the checkbox	on column L or R
S D 🔒 Acti	vity Timestamp	E Tinestemp	Principal
	Left click, hold, drag to	reposition column L or R	
Timestamp		Timestamp	\ ≜
Click on the colum	n header to sort Ascendir	ng or Descending (not all colum	nns 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 $\frac{1}{100}$ icon on the filter above the table view or click the $\frac{1}{100}$ 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.

Tags	Enter text	
Comments	NO VALUE	O _S
Match	Default	Search Tables
Date of Visit	molly	Columns
Page Title	samsh	Deselect All
URL		Filter
User Account		
No of Visits		Tags
URL Typed?		Comments
URL Status		Classifier
URL Type		



Click the Apply button to apply the filter.

Filter Apply Button					
	APPLY				

Active Filters are shown next to the column name that has been filtered (represented by the $\overline{\mbox{\sc icon}}$). The filter can be removed by clicking on that icon.

Active Filters				
	URL			
	User Name			
	No of Visits			
	URL Typed?			
	URL Status			
	URL Type	2		
	-			

Active filters are also shown on the top of the columns with the $\sqrt{3}$ icon. These filters can be removed by clicking on that icon.

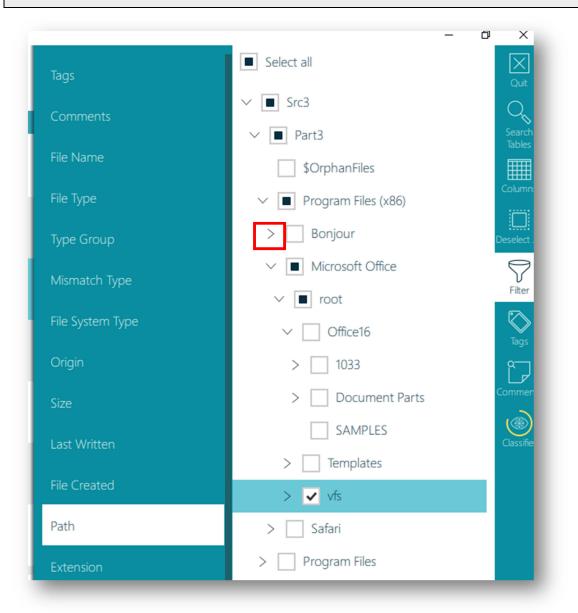
Active Filters						
Browsing History	User Name	URL Typed?	URL Type			
🔯 🄁 🕵 Date of Visit	t	Page Title		URL		



Filtering by Path

Enables the filtering of displayed files by path.

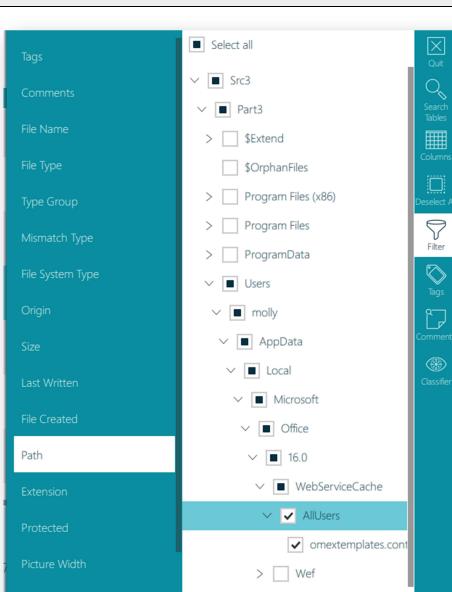
1. Clicking the Path option allows the results to be filtered by path. A selected folder indicates that all the items within that folder and any sub folders are selected. A black check box indicates a partial selection. Clicking the > icon will display sub folders.





2.

When the desired folders have been s	selected click on Appl	y
--------------------------------------	------------------------	---



OneDrive

Windows

Opera Software

(i) Details

Mozilla

>

>

>

>



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	
Size	Select all	Quit
Last Written	✓ □ Src3	Q
File Created	✓ Part3	Search Tables
Path	> \$Extend \$OrphanFiles	Columns
Extension	 Program Files (x86) 	
	> Program Files	
Protected	> ProgramData	Filter
Picture Width	✓ □ Users	Tags
Picture Height	✓ ☐ molly	
Video Duration	✓ ☐ AppData	Comments
Linked Artifacts	✓ □ Local	Classifier
Photo Probability	✓ Microsoft	
	✓ Office	
Visual Class	✓ □ 16.0	
EXIF Make	✓ WebServiceCache	
EXIF Model	AllUsers omextemplates.com	
EXIF Camera Serial Number	> Wef	
EXIF Date Time	> OneDrive	
EXIF Coordinates	> Windows	
Auto-Tagged	> Mozilla	
	> Opera Software	
Match		(i) Details
Captures	APPLY	



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.

, follow	Preset probability values	
Picture Width	Low Medium High	
Picture Height	Greater than or equal to	
Video Duration	Lower than or equal to	
Linked Artifacts		
Photo Probability	Desele	
Visual Class	U Filte	er
Entities	<u>≮`</u> Zoo	> m
EXIF Make	Tag	>
EXIF Model		, ,
EXIF Camera Serial Number	Comm	
EXIF Date Time	Class	
EXIF Coordinates		
Auto-Tagged	(i)
Captures	APPLY	



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					
Tags		Bestiality	0 100 100	Quit	
Comments		Child Abuse	85 100 0 100	Search Tables	
Hash Deduplicatio	1	Currency	85 100 0 100	Columns	
File Name			85 100	Deselect All	
File Type		Others	0 100 85 100	Filter	
Type Group		People	0 100	Zoom	
Mismatch Type		Pornography	0 100 100	Tags	
File System Type Origin		Portrait	0 100	Comments	
Size		Scanned Doc	85 100 0 100	Classifier	
Last Written		Upskirting	85 100 0 100	CROSSINC	
File Created		opskirting	85 100		
Path		Vehicle	0 100 85		
Extension		Weapon	0		
Protected					
Picture Width					
Picture Height					
Video Duration					
Linked Artifacts					
Photo Probability					
Visual Class	2				

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				
	Pictures classification Classification in progress. Please wait Pictures classified 16/47 Potential matches (with at least 85% confidence) Portrait 1 Scanned Doc 1 Video classification Classification paused. Video classified 0/8	Qut Qut Bables Classifier	Pictures classification Classification completed. Pictures classified 47/47 Potential matches (with at least 85% confidence) Others 1 Portrait 1 Scanned Doc 4 Video classification Classification paused.	Qut Qut Search Tables Cassifier
			Videos classified 1/8 Potential matches (with at least 85% confidence) Others 1	
	PAUSE		RESUME	1

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
Date of Visit ↑ <u>≐</u>	Date of Visit ↓ =

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
		Sto	iNode1669281	Portable Network Graphic	Picture
1.	Select one record - S	Single click	or by pressing	the space bar	

- 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

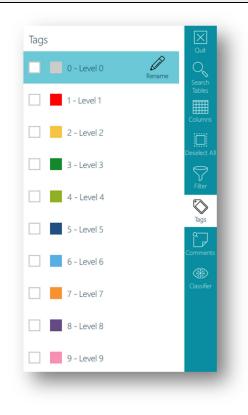


 Navigation between records can also be achieved using: Arrow keys (left -right-up-down) Scroll bar Mouse scroll wheel

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.

 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.

- 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
- 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.

K lose	$\leftarrow \rightarrow$	SUMMARY					Qui
nary	Enter text			<u> </u>			Sear Tabl
ures S	SCAN INFO	ORMATION	SEARCH	PROFILE	STATISTIC	S	Class
eos	Scan Name	Scan 2018-10-05 09-53-29	Name	Comprehensive - General Profiling	Scan Duration	0h 21m 15s	
≤	Scan Date Scan Time System	2018-10-05 09:53:30 2018-10-05	Notes	Comprehensive scan - CAUTION - all videos files are	Status Files Collected	Completed 7483	

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.



$\leftarrow \rightarrow$ Files						Records: Selected: Tags:	181593
canon		Q	< 1/2 >				(S T
> Microsoft." > Microsoft.	Vekyb3d8bbwe Vekyb3d8bbwe Wekyb3d8bbwe	Excerpts	Preview readed Not created	File Name FRE_OUTRO_ULW ma music_Neutral_01_ PRE_OUTRO_02.W ma SongsAndThemes, json	File Type Advanced Systems Format Microsoft Advanced Systems Format	Type Group Video	Ca Des
✓ Microsoft.' ✓ AppCS Assets APPL'	Wekyb3d8bbwe	•		AGMBackground.j pg AlbumsOverrideB ackground.jpg	JPEG/JIFF Image	Picture Picture	Cor Ca
Properties Make Model Senial Number Date Time Dipitized ApertureValue ApplicationRecordVersion BitsPerSample ColarSpace	Metadata Cancel Cancel EOS 7D 0281724837 2015:12:13 12:23:28 F2:8 4 8 8 8 8 88 8 88 8 86	Preview					Since of the second sec
Comment CustomRendered		nini 3.13.3.2TB 0x07b6cefb					(

3. 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.

	FILES							Selected: 1 Tags:
2014/11/25		O _N						1
Select all		\diamond	Excerpts	Preview	File Name	File Type	Type Group	Mismatch Type
	wpnidm	-						Der
S	PRICache			28	54f19a1.jpg	JPEG/JIFF Image	Picture	
	SettingSync			a				
	Shell				fddf008b.jpg	JPEG/JIFF Image	Picture	
	Themes			2 D				
		- □			1568834.jpg	JPEG/JIFF Image	Picture	
	UPPS							
	WER				76e05dd2.jpg	JPEG/JIFF Image	Picture	a
	WebCache							_
>	WinX				4a5315c.jpg	JPEG/JIFF Image	Picture	
	APPLY							
Properties	Metadata	Preview						-
Preview				File Name	bba5f105.jpg			Uncock Open with
File Type	JPEG/JIFF Image			Type Group	Picture			
File System Type	File			Origin	Allocated			Save as
Size	5585			Last Written	2014/11/25 21:27:33			
File Created	2014/11/25 21:27:33			Last Accessed	2014/11/25 21:27:33			
Path	Src5/Part2/Users/ADF Test/App	Data/Local/Micro	oft/Windows/Notifi					
Extension	jpg			Protected	Not protected			
Picture Width	210	50545		Picture Height	173			
Integrity MD5	86A7D39B112EE23262BEF2B0110	59FAE		Integrity SHA1	4F27HZZ3ZT2SBB5KCF	UNMG6PNWHK2AYB		





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 Viev	v		
Digital Evidence Inves	tigator			↔	
$\leftarrow \rightarrow$	TIMELINE			Records: Selected Activities: Tags:	23751 1
Ö (🗍 🖳 Timestamp 🔍	Activity	Info	Preview	
	16:26:15 (L)	visited			
	2018/01/24	Recent access	catalan-		
	16:26:15		sheepdog-2.jpg		
	2018/01/24	File created	catalan-		De
	16:26:15		sheepdog-2.jpg		
	2018/01/24	Last written	catalan-		
	16:26:15		sheepdog-2.jpg		
	2018/01/24	Browser URL			
	16:26:06	visited			Co
	2018/01/24	Recent access	catalan-		
	16:26:06		sheepdog-3.jpg		
					_
Properti					
Target	catalan-sheepdog-2.jpg	Is Folder	No		
Extension	jpg	File Type	Picture		
User Account	samsh	Path		nsh\OneDrive\Go	spix\
Drive Type	Fixed	Volume S	erial 28A889C7		
Date Accessed	2018/01/24 16:26:15				
Candidate	Src21/Part3/Users/samsh, [Referenced Files]	/OneDrive/Gospix/cata	lan-sheepdog-2.jpg		
	[Pictures Comprehensive	Thorough ID no carvin	ig]		
Source	Microsoft Windows				
Source File	Src21/Part3/Users/samsh, sheepdog-2.lnk	/AppData/Roaming/Mi	crosoft/Windows/Re	cent/catalan-	
Source Details	No details	Auto-Tagg	ged No		
	Decent Files				

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.

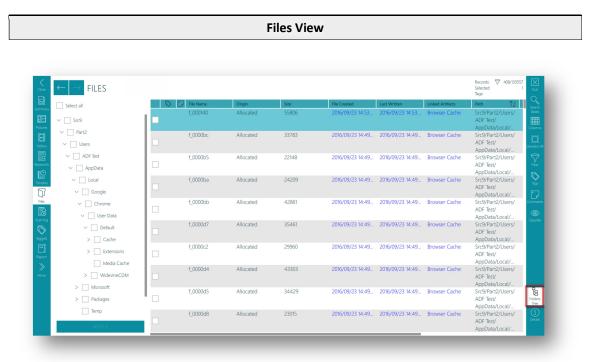
Timeline records that relate to a file may contain, within the Details view of that file, a hyperlink to the Files View filtered by the path of the file concerned.



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 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		
\leftarrow \rightarrow Messages				
🛇 🏳 <u>&</u> Excerpts	Message Thread	Message	Attachment Name	Date/Time ↓=
	7	Unread message 100220-1606 447452938009 (Martin Mulholand) - 16:06:10		2020/02/10 16:06
	7	Snow lying now 447452938009 (Martin Mulholand) - 16:02:32	15813505528674 [Referenced Files] [Pictures and Vi	2020/02/10 16:02
	7	Group message from Martin 100220-1602 447452938009 (Martin Mulholand) - 16.02-03		2020/02/10 16:02
	7	Group message from Tom 100220-1601 447493764850 (Tom) - 16:01:02		2020/02/10 16:01:
	7	Group message from James 100219-1600 447452938011 (James McLevy) - 16:00:22		2020/02/10 16:00
	7	408072901786790658 447452938011 (James McLewy) - 15:59:39		2020/02/10 15:59
	7	Test Viber Group 447452938011 (James McLew) - 15:59:15		2020/02/10 15:59
	7	Test Group 447452938011 (James McLew) - 15:58:50		2020/02/10 15:58

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



		Excerpts	Preview	File Name	File Type	Type Group	Mismatch Type	Origin	Q
, 📃 0 - Level				Scenario5RTL.png				Allocated	Table
1 - Level		5			Graphic				Colum
3 - Level				7e61214d.jpg	JPEG/JIFF Image	Picture		Allocated	
4 - Level		5							Deselec
5 - Level		5		43206eb7.jpg	JPEG/JIFF Image	Picture		Allocated	5
FILES		6							Filte
User I	Logins 3								No.
📕 6 - Level									
📕 7 - Level									Comme
8 - Level									œ
9 - Level									Classif
Properties	Preview								
								1 Linear	
Properties Tags	Preview 5 - Level 5		Pre	iew 🎫					
					Network Graphic				
Tags	5 - Level 5		File		Network Graphic			Unosci Gren with Same as	
Tags File Name	5 - Level 5 Scenario5RTL.png		File	Type Portable System Type File	Network Graphic				
Tags File Name Type Group	5 - Level 5 Scenario5RTL.png Picture		File Size	Type Portable System Type File 173516	Network Graphic 3 10:51:08				
Tags File Name Type Group Origin	5 - Level 5 Scenario5RTL.png Picture Allocated		File Size	Type Portable System Type File 173516					
Tags File Name Type Group Origin Last Written	5 - Level 5 Scenario5RTL.png Picture Allocated 2017/10/13 10:52:08 2017/10/13 10:51:08	/WindowsApps/Microsoft.3D	File File Size File	Type Portable System Type File 173516 Created 2017/10/1 kyb3d8bbwe/Assets/Her	13 10:51:08 roHelp				
Tags File Name Type Group Origin Last Written Last Accessed	5 - Level 5 Scenario5RTL.png Picture Allocated 2017/10/13 10:52:08 2017/10/13 10:51:08	/WindowsApps/Microsoft3D	File File Size File Builder_14.1.1302.0_x868we Prov	Type Portable System Type File 173516 Created 2017/10/1	13 10:51:08 roHelp				(1) Detail

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.

Properties	Preview	Duplicates	
Src6/Part2/Users/ADF	Test/AppData/Local/	Packages/Microsoft.Microso	tEdge_8wekyb3d8bbwe/AC/#!001/MicrosoftEdge/Cache/5LJC3US1/chrome-dial-pointer.310172ec[1].png

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				
	Hide duplicates			
Tags Comments				
Hash Dedupikation				
March File Name	Course of			
File Type Type Group				
Mamatch Type				
File System Type Origin				
Size	Course			

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

	Zone in Summary View		
$\leftarrow \rightarrow SU$	MMARY		
SCAN INFORMA	ATION		
Scan Name	Win10_CompGPsopt		
Scan Date	2018-09-14		
Scan Time	10:05:15		
System Date	2018-09-14		
System Time	10:05:15		
Viewer Time Zone	Europe/London		

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.



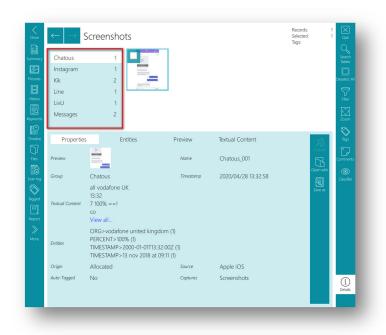
Reviewing Screenshots

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

	\leftarrow \rightarrow Screenshots				1 X 1 Quit
nary Chatous	1				Search Tables
Instagram	1				
^{ires} Kik fil	2	And Tana a			Deselect All
Line	1				Filter
LivU	1				
ords	2				Zoom
eine Properties	s Entities	Preview	Textual Content	A.	Tags
			ickladi content	Undock	ۍ ۲
es Preview		Name	Instagram_001	5	Comments
Group	Instagram	Timestamp	2020/04/28 13:34:41	Open with	Classifier
	e			Save as	
ged	oda Oo	Entities	PLACE>aa (1)		
Nort	V		PLACE>ny (1)		
Origin	View all Allocated	Source	Apple iOS		
Auto-Tagged	No	Captures	Screenshots		
					í



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

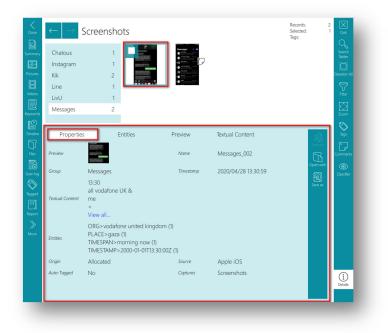


2. Clicking on a Screenshot Group name will show a gallery of screenshots taken under that name

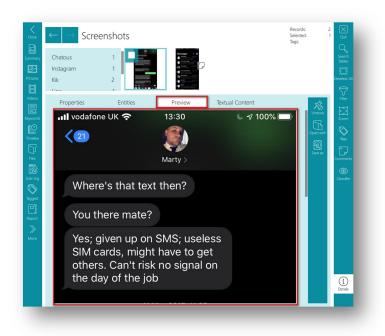




3. Clicking on a screenshot in the gallery will update the Details pane. The Properties tab will show details associated with the screenshot such as the name, the date/time the screenshot was taken and any user entered comments

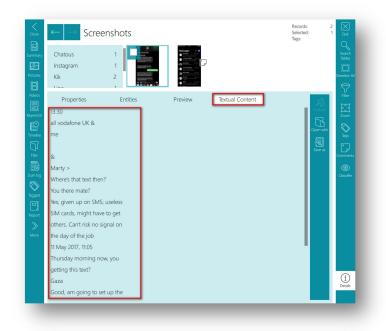


4. The Preview tab will show a full size image of the screenshot





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.

							View							_
\leftarrow \rightarrow Create Ref	ORT													Qut
Format			٦.			Option	s							1
	vics os	tandalone viewer	1		2	Path*	:\Users\Stuar	t\Desktop\Sca	an 2018-08-28	11-58-50				
Content Selection			_			_								4
Content selection														
All records	✔ 0 - Le	wel 0 🖌 1 - Lev	el 1 🗸 2 - Le	vel 2 🗸 3 - Le	vel 3 🖌 4 - Lev	rel 4 🗸 5 - Le	vel 5 🖌 6 - Lev	vel 6 🗸 7 - Lev	vel 7 🖌 8 - Lev	el 8 🖌 9 - Le	vel 9 No tag	Include	e ori List layout	1
SUMMARY														
APPLICATIONS>Anti-Forensics	Tr										152			
APPLICATIONS>Application U	sage										26			
APPLICATIONS>Installed Appl	ica										24			
APPLICATIONS>P2P Traces											3			
COMMUNICATION > Calls											3			
COMMUNICATION > Messages											45			
COMMUNICATION > Saved Co	nt										5			
COMMUNICATION>Skype - N	le					3					1			
COMMUNICATION > Skype Rei	:ei	✓ 1									7	~		
DEVICE DATA>OS Information											1			
DEVICE DATA>USB History											11			
DOCUMENTS>Referenced File	IS		✔ 1							✔ 1	11	~		
IPOC>IPOC - Keywords Comp	re	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	179			
MULTIMEDIA>Pictures Compr	eh 🗹 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✔ 1	✓ 1	748			
MULTIMEDIA>Videos under 10	10													
USER DATA>Recent Files											44			
USER DATA>User Accounts											6			
WEB BROWSERS>Browsing H	st										3396			
WEB BROWSERS>Search Term	IS										143			
TIMELINE	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	4256	~		
FILES	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	1857			
SCAN LOG											108			
						EXPORT			4					

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.

← → CREATE REPORT													
Format						Options							
HTML OPDF OCSV OVICS	Standa	lone viewer				Path* C:\	Users\Stuart\[Desktop\Scan	2018-08-28 11	-58-50			
Content Selection													
All records	0 - Level 0	✓ 1 - Level 1	2 - Leve	2 🖌 3 - Level 3	3 🖌 4 - Level 4	4 🗸 5 - Level	5 🖌 6 - Level	5 🗸 7 - Level 1	7 🗸 8 - Level	8 🔽 9 - Level 9	No tag	Indude ori	List layout
SUMMARY													
APPLICATIONS>Anti-Forensics Tr											152		
APPLICATIONS>Application Usage											26		
APPLICATIONS>Installed Applica											24		
APPLICATIONS>P2P Traces											3		
COMMUNICATION>Calls											3		
COMMUNICATION>Messages											45		
COMMUNICATION>Saved Cont											5		
COMMUNICATION>Skype - Me											1		
COMMUNICATION>Skype Recei		✓ 1									7	~	
DEVICE DATA>OS Information											1		
DEVICE DATA>USB History											11		
DOCUMENTS>Referenced Files			✔ 1							✓ 1	11	~	
IPOC>IPOC - Keywords Compre		✓ 1	✓ 1	✔ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	179	~	
MULTIMEDIA>Pictures Compreh	1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	748	~	
MULTIMEDIA>Videos under 100											3		
USER DATA>Recent Files											44		
USER DATA>User Accounts											6		
WEB BROWSERS>Browsing Hist											3396		
WEB BROWSERS>Search Terms											143		
	1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	4256	~	
FILES	1	✓ 1	√ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	1857	~	
SCAN LOG											108		



- 2.
- Select Format HTML from the format section.

Format						Options							
	○ Stand:	lone viewer					Users\Stuart\	Desktop\Scan	2018-08-28 1	-58-50			
	O Didition												
Content Selection													
All records	0 - Level 0	✓ 1 - Level	1 🗸 2 - Leve	12 🗸 3 - Level	3 🗸 4 - Leve	14 🗸 5 - Lew	el 5 🔽 6 - Leve	16 🗸 7 - Leve	17 🖌 8 - Levi	18 🗸 9 - Lev	si 9 📃 No ta	g 📕 Include of	ri List layout
SUMMARY													
APPLICATIONS>Anti-Forensics Tr											152		
APPLICATIONS>Application Usage											26		
APPLICATIONS>Installed Applica											24		
APPLICATIONS>P2P Traces											3		
COMMUNICATION>Calls											3		
COMMUNICATION > Messages											45		
COMMUNICATION>Saved Cont											5		
COMMUNICATION>Skype - Me											1		
COMMUNICATION>Skype Recei		✓ 1									7	~	
DEVICE DATA>OS Information											1		
DEVICE DATA>USB History											11		
DOCUMENTS>Referenced Files			✓ 1							✓ 1	11	~	
IPOC>IPOC - Keywords Compre		√ 1	✓ 1	√ 1	✔ 1	✓ 1	✔ 1	✓ 1	✓ 1	✓ 1	179	~	
MULTIMEDIA>Pictures Compreh	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✔ 1	✓ 1	✓ 1	✓ 1	748	~	
MULTIMEDIA>Videos under 100											3		
USER DATA>Recent Files											44		
USER DATA>User Accounts											6		
WEB BROWSERS>Browsing Hist											3396		
WEB BROWSERS>Search Terms											143		
TIMELINE	✓ 1	✓ 1	✓ 1	✓ 1	✔ 1	✓ 1	✓ 1	✓ 1	✔ 1	✓ 1	4256	~	
FILES	v 1	✔ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	1857	~	
SCAN LOG											108		

3.

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

ormat						Options							
	S O Star	dalone viewer				Path* C	\Users\Stuart	Desktop\Scan	2018-08-28 11	-58-50			
Content Selection													
All records	✓ 0 - Leve	10 🗸 1 - Lev	el 1 🗸 2 - Les	el 2 🗸 3 - Lev	el 3 🗸 4 - Lev	vel 4 🗸 5 - Lev	rel 5 🔽 6 - Lev	el 6 🗸 7 - Levi	el 7 🗸 8 - Leve	18 🗸 9 - Level !	9 No ta	Include ori	List layout
SUMMARY													
APPLICATIONS>Anti-Forensics Tr											152		
APPLICATIONS>Application Usage											26		
APPLICATIONS>Installed Applica											24		
APPLICATIONS>P2P Traces											3		
COMMUNICATION > Calls											3		
COMMUNICATION>Messages											45		
COMMUNICATION > Saved Cont											5		
COMMUNICATION>Skype - Me											1		
COMMUNICATION > Skype Recei		✓ 1									7	~	
DEVICE DATA>OS Information											1		
DEVICE DATA>USB History											11		
DOCUMENTS>Referenced Files			✓ 1							✓ 1	11	~	
IPOC>IPOC - Keywords Compre		✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	179	~	
 MULTIMEDIA>Pictures Compreh 	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	748	~	
MULTIMEDIA>Videos under 100											3		
USER DATA>Recent Files											44		
USER DATA>User Accounts											6		
WEB BROWSERS>Browsing Hist											3396		
WEB BROWSERS>Search Terms											143		
TIMELINE	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	4256	~	
 FILES 	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	1857	~	
SCAN LOG											108		



4	
4	
-	

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

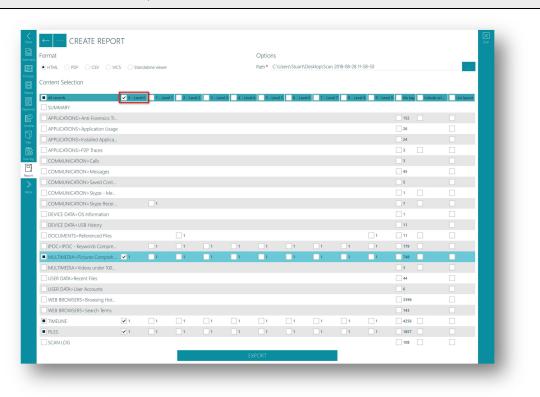
CREATE REPOR	т												
Format						Options							
	Stand	alone viewer				Path* C:\l	Jsers\Stuart\D	esktop\Scan 2	018-08-28 11-	-58-50			
tures													
Content Selection													
All records	✓ 0 - Level 0	🖌 1 - Level	1 🖌 2 - Leve	12 🗸 3 - Level	3 🗸 4 - Level	4 🗸 5 - Level	5 🖌 6 - Level	6 🗸 7 - Level	7 🖌 8 - Level	8 🖌 9 - Level	9 🖌 No ta	g 📕 Include ori.	List layout
All records													
APPLICATIONS>Anti-Forensics Tr											✓ 152		
APPLICATIONS>Application Usage											✔ 26		
APPLICATIONS>Application Usage											✔ 24		
APPLICATIONS>P2P Traces											✔ 3		
COMMUNICATION>Calls											✔ 3		
COMMUNICATION > Messages											✔ 45		
COMMUNICATION>Saved Cont											✔ 5		
COMMUNICATION>Skype - Me											✓ 1		
COMMUNICATION>Skype Recei		✓ 1									✓ 7	~	
DEVICE DATA>OS Information											✓ 1		
✓ DEVICE DATA>USB History											✓ 11		
DOCUMENTS>Referenced Files			✓ 1							✓ 1	✓ 11	~	
✓ IPOC>IPOC - Keywords Compre		✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 179	~	
MULTIMEDIA>Pictures Compreh	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✔ 748	~	
MULTIMEDIA>Videos under 100											✓ 3		
✓ USER DATA>Recent Files											✔ 44		
✓ USER DATA>User Accounts											✓ 6		
✓ WEB BROWSERS>Browsing Hist											✔ 3396		
✓ WEB BROWSERS>Search Terms											✓ 143		
✓ TIMELINE	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✔ 4256	~	
✓ FILES	√ 1	✓ 1	✓ 1	√ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1857	~	
SCAN LOG											✓ 108		
				_	_ E)	(PORT	_	_					

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

Format						Options							
	ICS O Sta	indalone viewer				Path* C	:\Users\Stuart	\Desktop\Scar	2018-08-28	11-58-50			
Content Selection													
 All records 	0 - Les	el 0 🔳 1 - Lev	el 1 🔳 2 - Le	rel 2 🔳 3 - Le	vel 3 🔳 4 - Le	vel 4 🔳 5 - Le	vel 5 🔳 6 - Le	vel 6 🔳 7 - Lev	el 7 🔳 8 - Le	vel 8 🔳 9 - Le	vel 9 🔳 No ta	ig Include	ori List layout
SUMMARY													
APPLICATIONS > Anti-Forensics Tr											152		
APPLICATIONS> Application Usag	e										26		
APPLICATIONS>Installed Applica											24		
APPLICATIONS>P2P Traces											3		
COMMUNICATION > Calls											3		
COMMUNICATION>Messages											45		
COMMUNICATION>Saved Cont.											5		
COMMUNICATION>Skype - Me											1		
COMMUNICATION> Skype Recei.		1									7		
DEVICE DATA>OS Information											1		
DEVICE DATA>USB History											11		
DOCUMENTS>Referenced Files			1							1	11		
IPOC>IPOC - Keywords Compre.		1	1	1	1	1	1	1	1	1	179		
 MULTIMEDIA>Pictures Compreh. 	. 🗹 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 748		
MULTIMEDIA>Videos under 100											3		
USER DATA>Recent Files											44		
USER DATA>User Accounts											6		
WEB BROWSERS>Browsing Hist.											3396		
WEB BROWSERS>Search Terms											143		
TIMELINE	1	1	1	1	1	1	1	1	1	1	4256		
FILES	1	1	1	1	1	1	1	1	1	1	1857		
SCAN LOG											108		
						EXPORT							



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



7.

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

Format						Options							
	S 🔿 Stan	dalone viewer				Path* C	\Users\Stuart	\Desktop\Scan	2018-08-28 1	1-58-50			
Content Selection													
All records	0 - Level	0 1 - Leve	1 2 - Ley	el 2 3 - Le	/el 3 4 - Lev	el 4 5 - Le	rel 5 6 - Les	rel 6 7 - Leve	17 8 - Lev	el 8 9 - Level	9 No ta	🖌 🖌 Include ori.	. List layout
SUMMARY								_					
APPLICATIONS>Anti-Forensics Tr											152	~	
APPLICATIONS>Application Usage											26		
APPLICATIONS>Installed Applica											24		
APPLICATIONS>P2P Traces											3	~	
COMMUNICATION > Calls											3		
COMMUNICATION>Messages											45		
COMMUNICATION>Saved Cont											5		
COMMUNICATION>Skype - Me											1	~	
COMMUNICATION>Skype Recei		1									7	~	
DEVICE DATA>OS Information											1		
DEVICE DATA>USB History											11		
DOCUMENTS>Referenced Files			1							1	11	~	
IPOC>IPOC - Keywords Compre		1	1	1	1	1	1	1	1	1	179	~	
MULTIMEDIA>Pictures Compreh	1	1	1	1	1	1	1	1	1	1	748	~	
MULTIMEDIA>Videos under 100											3	~	
USER DATA>Recent Files											44		
USER DATA>User Accounts											6		
WEB BROWSERS>Browsing Hist											3396		
WEB BROWSERS>Search Terms											143		
TIMELINE	1	1	1	1	1	1	1	1	1	1	4256	~	
FILES	1	1	1	1	1	1	1	1	1	1	1857	~	
SCAN LOG											108	~	
						EXPORT							



8.

Optional - Select the checkbox to have a list layout instead of table layout within the report.

Format						Options							
	CS O Standak	ne viewer				Path* C:\Us	ers\Stuart\De	sktop\Scan 20	18-08-28 11-58-	50			
Content Selection													
Jontent Selection													
All records	0 - Level 0	1 - Level 1	2 - Level 2	3 - Level 3	4 - Level 4	4 5 - Level 5	6 - Level 6	7 - Level 7	8 - Level 8	9 - Level 9	No tag	Include ori	 List layout
SUMMARY													
APPLICATIONS>Anti-Forensics Tr													~
APPLICATIONS>Application Usage	2										26		~
APPLICATIONS>Installed Applica.											24		~
APPLICATIONS>P2P Traces											3		~
COMMUNICATION>Calls											3		~
COMMUNICATION > Messages											45		~
COMMUNICATION>Saved Cont											5		v
COMMUNICATION>Skype - Me											1		~
COMMUNICATION>Skype Recei		1									7		~
DEVICE DATA>OS Information											1		~
DEVICE DATA>USB History											11		~
DOCUMENTS>Referenced Files			1							1	11		~
IPOC>IPOC - Keywords Compre		1	1	1	1	1	1	1	1	1	179		~
MULTIMEDIA>Pictures Compreh	1	1	1	1	1	1	1	1	1	1	748		~
MULTIMEDIA>Videos under 100											3		~
USER DATA>Recent Files											44		~
USER DATA>User Accounts											6		~
WEB BROWSERS>Browsing Hist											3396		~
WEB BROWSERS>Search Terms											143		~
TIMELINE	1	1	1	1	1	1	1	_ 1	1	1	4256		~
FILES	1	1	1	1	1	1	1	1	1	1	1857		~
SCAN LOG											108		~

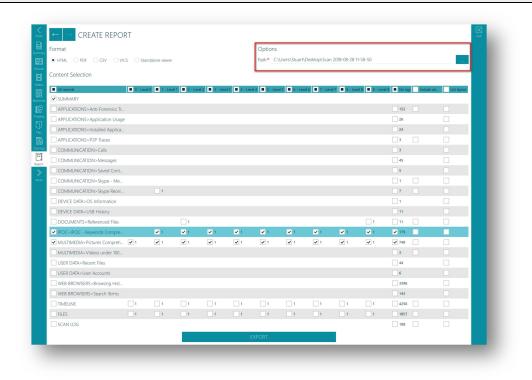
9.

Optional - Select the checkbox to have a Summary page included within the report.

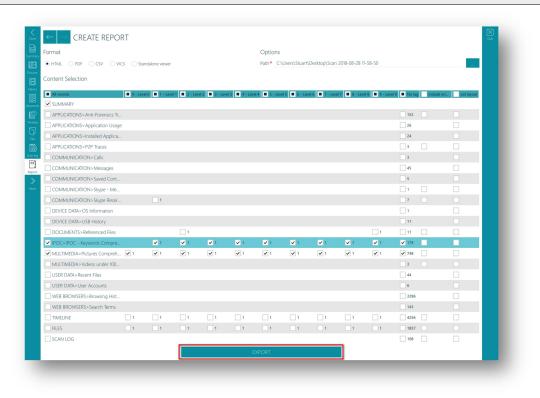
Format						Options							
	vics 🔿	Standalone viewer				Path* C	:\Users\Stuart	\Desktop\Scar	n 2018-08-28	11-58-50			
Content Selection													
All records	0 -	Level 0 1 - Leve	1 2 - Le	vel 2 3 - Le	vel 3 4 - Le	vel 4 5 - Le	vel 5 🚺 6 - Le	vel 6 📃 7 - Lev	vel 7 🔡 8 - Le	vel 8 📃 9 - Le	vel 9 No ta	g Include c	ri List layout
SUMMARY													
APPLICATIONS > Anti-Forensics T											152		
APPLICATIONS>Application Usa	ge										26		
APPLICATIONS>Installed Applica											24		
APPLICATIONS>P2P Traces											3		
COMMUNICATION>Calls											3		
COMMUNICATION>Messages											45		
COMMUNICATION>Saved Cont											5		
COMMUNICATION>Skype - Me											1		
COMMUNICATION>Skype Rece		1									7		
DEVICE DATA>OS Information											1		
DEVICE DATA>USB History											11		
DOCUMENTS>Referenced Files			1							1	11		
IPOC>IPOC - Keywords Compre		1	1	1	1	1	1	1	1	1	179		
MULTIMEDIA>Pictures Compreh	🗌 1	1	1	1	1	1	1	1	1	1	748		
MULTIMEDIA> Videos under 100.											3		
USER DATA>Recent Files											44		
USER DATA>User Accounts											6		
WEB BROWSERS>Browsing Hist											3396		
WEB BROWSERS>Search Terms											143		
TIMELINE	1	1	1	1	1	1	1	1	1	1	4256		
FILES	1	1	1	1	1	1	1	1	1	1	1857		
SCAN LOG											108		
						EXPORT	_						



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.





Opening HTML Report

HTML reports are stored within a folder as specified within the Option path field. To open an HTML report, browse to the location where the folder was created, open the folder and double click on the *index.html* file therein:

Name	Date modified	Туре
📕 html_pages	29/08/2018 10:41	File folder
previews	29/08/2018 10:41	File folder
🗹 📀 index.html	29/08/2018 10:41	Chrome HTML Document
		,

When viewing an HTML report it will open within the default web browser.

The HTML report displays the same columns that were visible in the viewer in the order they were displayed. To remove columns from the HTML report hide them within the viewer prior to creating the report. A navigation bar appears when moving the cursor over the turquoise section at the left-hand side of the report containing the >> symbol.

FILES	1	H PROF	LE		STATISTI	cs			TAGS STATIST	TICS		î.
		ор	timized	sive - IPOC speed sive scan - Runs all	Scan Durat Status Files Collec	on Oh Om 29s Completed			0 - Level 0 1 - Level 1 2 - Level 2	i i		- 8
		art	ifact Cap bedded,	tures, collects allocated, and deleted pictures	Application		Evidence Invest	igator	3 - Level 3 4 - Level 4			- 8
		IP	DC keywo	searches for common ords, and searches for or values using the					5 - Level 5 6 - Level 6 7 - Level 7			- 8
		W	thout Ext	dentification for Files ension option. Searches ensics traces, remote					8 - Level 8 9 - Level 9			- 8
		ac fro	cess trace m Skype	es, P2P traces and files caches. Collects								
			otected fi ocessed k	les and files not by parser								- 8
												- 8
Messages		4		DEVICE DATA		DOCUM	ENTS		IPOC			- 8
		3 0	S	Connection Log Device Information	0	Reference	d Files	13	IPOC - Hash Comprehen optimized		0	- 8
		45 5	6	OS Information USB History					IPOC - Keyv Comprehen		886	- 8
MULTIMEDIA>Pictures Comprehensive - speed optimized		1							optimized			- 8
		8										- 10
		0		WEB BROWSERS								- 11
		44 6		Browsing History Download History	0							- 11
		0		Search Terms	143							- 8
												- 8



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.

														Quit
← → CREATE REF	ORT													Quit
Format						Options	5							
	VICS OSta	indalone viewei				Path* C	:\Users\Stuart	t\Desktop\Sca	in 2018-08-28	11-58-50 PDF			· · · · ·	1
						Orientatio	on: Landso 	cape O Port	trait					
Content Selection														
All records	0 - Lev	el 0 🔳 1 - Lev	rel 1 🔳 2 - Le	vel 2 🔳 3 - Le	wel 3 🔳 4 - Le	evel 4 🔳 5 - Le	rvel 5 🔳 6 - Le	vel 6 🔳 7 - Le	rvel 7 🔳 8 - Le	vel 8 🔳 9 - Le	vel 9 🔳 No ta	Include	e ori List layour	1
SUMMARY														
APPLICATIONS>Anti-Forensics	Tr										152	~		
APPLICATIONS>Application U	sage										26			
APPLICATIONS>Installed Appl	ica										24			
APPLICATIONS>P2P Traces											3	~		
COMMUNICATION>Calls											3			
COMMUNICATION > Messages											45			
COMMUNICATION > Saved Co	nt										5			
COMMUNICATION>Skype - N	1e										1	~		
COMMUNICATION>Skype Re	:ei	1									7	~		
DEVICE DATA>OS Information											1			
DEVICE DATA>USB History											11			
DOCUMENTS>Referenced File	is		1							1	11	~		
✓ IPOC>IPOC - Keywords Comp	re	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✔ 1	✓ 1	✓ 1	✓ 1	✓ 179	~		
MULTIMEDIA>Pictures Compr	eh 🔽 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✔ 748	~		
MULTIMEDIA>Videos under 10	0										3	~		
USER DATA>Recent Files											44			
USER DATA>User Accounts											6			
WEB BROWSERS>Browsing H	st										3396			
WEB BROWSERS>Search Term	IS										143			
TIMELINE	1	1	1	1	1	1	1	1	1	1	4256	~		
FILES	1	1	1	1	1	1	1	1	1	1	1857	~		
SCAN LOG											108	~		

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.

Options		- 1
	\Stuart\Desktop\Scan 2018-08-28 11-58-50 - PDF 3	



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:

	Openin	g PDF Repo	rt		
Name	Date modified 29/08/2018 14:01	Type PDF File	Size	3,300 KB	
	_	_	_	_	

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.

PDI	Report	
Scan 2018-08-28 11-58-50		
SUMMARY		
SCAN INFORMATION	SEARCH PROFILE	
Scan Birloha ATON Scan Diamo Scan 2016 00:211159-50 Scan Diamo 2016:00:21 Scan Diamo 2016:00:20 Spatem Diamo 2016:00:20 Spatem Diamo 2016:00:20 Spatem Time 11:05:01 Verver Time Europe/London STA110TC:5 Scan Duration Oh On 2% Status Completed Fluc Collected 805 Application AD Prolytals Foldence Investigator 0.00	CARCH PAOLE Cardina Paole Cardina Paole Cardina Paole Cardina Cardina Cardina Cardina Cardina Cardina Cardina Cardina Cardina Cardina Cardina Cardina	
CAPTURES APPLICATIONS And Growns 201 Toris 201 Application 24 Paper 201 Paper 201	COMMUNICATION Calls 3 S Emails 0 Messages 45 S Samed Contacts 5 S Syper - Roder 5 Styper Files 8 EDOCUMENTS	
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.

					CS	V Re	port					
												_
← → CREATE REPO	RT											Quit
Format						Options						
ry	cs 🔿 St	andalone viewer						t\Desktop\Sca	n 2018-08-28	11-58-50 - 2		
						_						
Content Selection												
All records	📕 0 - Le	vel 0 🔳 1 - Lev	rel 1 🔳 2 - Li	rvel 2 🔳 3 - Le	vel 3 🔳 4 - Lo	rvel 4 🔳 5 - Le	vel 5 🔳 6 - Le	vel 6 🔳 7 - Le	rel 7 🔳 8 - Le	vel 8 🔳 9 - Le	wel 9 🔳 No tag 📃 Indude ori	
APPLICATIONS>Anti-Forensics Tr.											152	
APPLICATIONS>Application Usage	9										26	
APPLICATIONS>Installed Applica.											24	
APPLICATIONS>P2P Traces											3	
COMMUNICATION > Calls											3	_
COMMUNICATION>Messages											45	
COMMUNICATION>Saved Cont											5	
COMMUNICATION>Skype - Me											1	
COMMUNICATION>Skype Recei		1									7	_
DEVICE DATA>OS Information											1	
DEVICE DATA>USB History											11	_
DOCUMENTS>Referenced Files			1							1	11	
✓ IPOC>IPOC - Keywords Compre		✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 179	_
✓ MULTIMEDIA>Pictures Compreh	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 748	_
MULTIMEDIA>Videos under 100											3	_
USER DATA>Recent Files											6	
											3396	_
WEB BROWSERS>Browsing Hist											143	
	1	1	1	1	1	1	1	1	1	1	4256	
FILES	1	1	1	1	1	1	1	1	1	1	1857	
											108	
						EVEODT						
						EXPORT						



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:

0	pening CSV Rep	ort	
Name	Date modified	Туре	Size
original files	20/09/2018 10:26	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
a PPLICATIONS-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
COUMENTS-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
Contraction Contraction Contraction Contraction	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
Contract Con	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.

					VIC	CS Re	epor	t								
Cose	← → CREATE REPOR	۲												X		
	Format					Options										
2		S Standalone	viewer			Path* C	:\Users\Stuart	\Desktop\Sca	n 2018-08-28	11-58-50 VICS	2					
Pare	Content Selection	-														
Videos	All records	🗸 0 - Level 0 🔳	1. Level 1 🔳 2.	Invel 2 2 3 - 1	and 3 🖌 d al	evel 4 1 5 - 1 e	uni 5 🖌 6 - 1 m	wi 6 🖌 7 - 14	uni 7 🖌 8 - 1 e	ool 8 🔳 9 - Leo	al 9 No.1	a 🖌 bachada e	wi	_		
Keywoods	COMMUNICATION>Skype - Me										1	~		-		
P	COMMUNICATION>Skype Recei		1								7	~				
Tendre	DOCUMENTS>Referenced Files		1							1	11					
CH Pie	MULTIMEDIA>Pictures Compreh	V 1 V	I 🔽 I	√ 1	V 1	✓ 1	✓ 1	✓ 1	✓ 1	V 1	748					
16	MULTIMEDIA>Videos under 100										3	~				
Scanlog																
8																
Report																
More																
						EXPORT										
			_													

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:

Name ^	Date modified	Туре	Size	
original files Scan 2018-08-28 11-58-50	29/08/2018 17:10 29/08/2018 17:10	File folder JSON File		2, 197 KB