



Search

Getting Started with Detective

The search process can search within files to uncover data that has not been parsed, often uncovering valuable data within SQLite databases, log files, and property lists. Investigators can search data according to the information entered in the input field, by keyword lists, hashes, using regular expressions or choosing any other available method.

All sections and analytics are laid out in a 3 column fashion across the board making it easier to find the information you are seeking. This document will walk you through which information will be found in each column.

The screenshot displays the Detective search interface with a search for 'jarparkers54@gmail.com'. The interface is divided into three main columns:

- COLUMN 1:** Search history and filters. The search history shows results for 11/6/2019, including searches for 'jarparkers54@gmail.com' and 'PatPayge'. The filters section includes sources like Contacts, Facebook, Google+, and WebKit Data.
- COLUMN 2:** Search results table. The search criteria is 'jarparkers54@gmail@[w.+%\\-]{0,25}\\.com'. The results table lists various items such as Contact, Appointment, and File, all associated with the email address 'jarparkers54@gmail.com'. The table has columns for Type, Values, Description, and Time stamp.
- COLUMN 3:** Details panel. It currently shows 'No information'.

Type	Values	Description	Time stamp
Contact	jarparkers54@gmail.com	Email: jarparkers54@gmail.com	
Appointment	jarparkers54@gmail.com	Attendees info: ...e: None; Name: jarparkers54@gmail.com, Email: jarparkers54@gmail.com, Status: I...	08/04/2011 03:00:00 PM
Contact	jarparkers54@gmail.com	Other: jarparkers54@gmail.com	
Contact	jarparkers54@gmail.com	Other: jarparkers54@gmail.com	
Contact	jarparkers54@gmail.com	Email: jarparkers54@gmail.com	
Contact	jarparkers54@gmail.com	Email: jarparkers54@gmail.com	
Contact	jarparkers54@gmail.com	Email: jarparkers54@gmail.com	
Contact	jarparkers54@gmail.com	Email: jarparkers54@gmail.com	
Contact	jarparkers54@gmail.com	Email: jarparkers54@gmail.com	
Contact	jarparkers54@gmail.com	Email: jarparkers54@gmail.com	
Contact	jarparkers54@gmail.com	Email: jarparkers54@gmail.com	
Contact	jarparkers54@gmail.com	User e-mail: jarparkers54@gmail.com	
Contact	jarparkers54@gmail.com	Email: jarparkers54@gmail.com	
Contact	jarparkers54@gmail.com	Email: jarparkers54@gmail.com	
Contact	jarparkers54@gmail.com	Email: jarparkers54@gmail.com	
File	jarparkers54@gmail.com	Name: _cookies_jarparkers54@gmail.com_facebook Full path: .../files/_cookies_jarparkers54@gmail.com_facebook	12/20/2012 09:57:00 AM
Account	jarparkers54@gmail.com	Email: jarparkers54@gmail.com	
Account	jarparkers54@gmail.com	Email: jarparkers54@gmail.com	



Column 1

Where: On the left-hand side of the Search section

Uses: This is your filter where you can narrow down the content by selection or deselection. Within this column you can choose what is to be viewed in Column 2 by unchecking or checking the boxes.

In the upper section of Column 1 you will find all of your search queries along with the number of results yielded.

The screenshot shows two sections of a mobile application interface. The top section is titled "Search history" and contains a search input field with the placeholder text "Enter text". Below the input field is a date separator "11/6/2019". The search history list includes the following entries:

Time	Search Query	Results
4:14 PM	jayparkers54@gmail[w....	16
4:08 PM	[Newset]	12
4:08 PM	[Newset], [IOS (System ...	25
4:04 PM	[PatPayge]	24
4:03 PM	[PatPayge] (Canceled)	333

The bottom section is titled "Filters" and shows a list of sources with checkboxes and result counts:

Source	Count
<input checked="" type="checkbox"/> Sources	16
<input checked="" type="checkbox"/> Contacts	7
<input checked="" type="checkbox"/> Dolphin Browser Mini	1
<input checked="" type="checkbox"/> Facebook	1
<input checked="" type="checkbox"/> Facebook Messenger	1
<input checked="" type="checkbox"/> Files	1
<input checked="" type="checkbox"/> Google Calendar	1
<input checked="" type="checkbox"/> Google+	1
<input checked="" type="checkbox"/> Phonebook	2
<input checked="" type="checkbox"/> WebKit Data	1

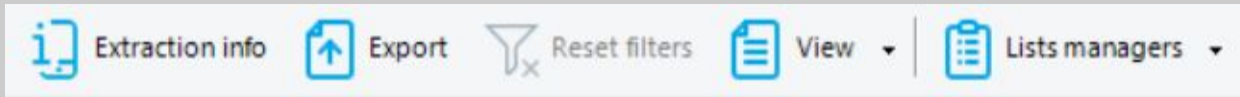
In the lower section of Column 1 you will see all of the sources from which your search results were pulled from.



Column 2

Where: In the center of the section.

Uses: This is your main grid column. Here is where you will see all the content that you have filtered down to on display.



The top bars above column 2:

- To move back to the device information click on the box “Extraction info”
- At the top of the screen is the “Export” function. Here is where you can form a selective report on the Search section. You will have the following formats to export your report to: PDF, XLSX, XML, HTML
- To clear out your filters there is a “Filters” button at the top of your screen above Column 2. If the “Clear filters” button is greyed out, this indicates that no filters are active and all available information in this section is being displayed.
- The “View” button allows you to control whether or not you see your tags, labels, thumbnails, and highlighted text displayed.
- The List Managers is a dropdown menu where you can choose Keyword lists, Hash Sets, and/or Regex lists that you’ve either imported or created in Detective. You can also search using regular text.



On the upper right-hand of the grid you will see a box labeled “Find text”. This is to filter through your grid to find specific characters. Once you start typing in your word to be filtered down to, you will see the filtered text start to highlight within the grid. If you press enter, your filtered content will be all that is displayed in the grid.



Once you are in the grid inside the section:

- The printer icon: Here is where you can select or deselect items to be included in your report.
- The star icon: This is a location to add items as key evidence. If the star is highlighted yellow, your item has been marked. I
- The tag icon: Once you start adding tags to your evidence items such as “Important” or “Not relevant” this is where you will start to see your labels show up. If you choose the box “Labels” in the “View” button as mentioned above, you will then not only see a color tag but will see what the tag has been named. This is also a filtering function drop down menu. You can filter to chosen tags only, if you need to do so. You can also arrange the types of tags in an ascending or descending order here.

Searching for Text: Search text using exact phrase or all words.

The screenshot shows the 'Text' search tab. At the top, there are tabs for 'Text', 'Keywords', 'Hash sets', and 'RegExp'. Below the tabs is an input field labeled 'Enter text'. Underneath is an 'Advanced settings' section with two dropdown menus: 'All text data' and 'Any words'. There are two checkboxes: 'Case sensitive' and 'Whole words only', both of which are unchecked. Below these are three checkboxes under the heading 'Search in': 'Parsed data', 'Files', and 'File content', all of which are checked.

Searching Keywords: Search any Keyword List that Detective already has on file, one that you've created, or imported.

The screenshot shows the 'Keywords' search tab. At the top, there are tabs for 'Text', 'Keywords', 'Hash sets', and 'RegExp'. To the right of the tabs is a search filter icon and the text 'Find text...'. Below the tabs is a dropdown menu labeled 'Select keywords'. To the right of this dropdown are two buttons: 'Keywords' and 'Search'. Underneath is an 'Advanced settings' section with two checkboxes: 'Case sensitive' and 'Whole words only', both of which are unchecked. Below these are three checkboxes under the heading 'Search in': 'Parsed data', 'Files', and 'File content', all of which are checked.

Searching Hash Sets: Search for known files by importing hash sets to run against device files.

The screenshot shows the 'Hash sets' search tab. At the top, there are tabs for 'Text', 'Keywords', 'Hash sets', and 'RegExp'. To the right of the tabs is a search filter icon and the text 'Find text...'. Below the tabs is a dropdown menu labeled 'Select hash set'. To the right of this dropdown are two buttons: 'Hash sets' and 'Search'.

Searching Regular Expressions: Use Detective's preset list or use a RegEx list of your own.

The screenshot shows the 'RegExp' search tab. At the top, there are tabs for 'Text', 'Keywords', 'Hash sets', and 'RegExp'. To the right of the tabs is a search filter icon and the text 'Find text...'. Below the tabs is an input field with the placeholder text 'Enter regular expression or select it from regexp manager'. To the right of this input field are two buttons: 'RegExp' and 'Search'. Underneath is an 'Advanced settings' section with three checkboxes under the heading 'Search in': 'Parsed data', 'Files', and 'File content', all of which are checked.








































Text Keywords Hash sets RegExp

Find text... ^ v

Select hash set v

Hash sets

Search

			Type	Hash set	Description	Time stamp
<input checked="" type="checkbox"/>			Image file "JPG"	 Newset	Name: 1351508337245.jpg	10/29/2012 01:58:00 PM
<input checked="" type="checkbox"/>			Image file "JPG"	 Newset	Name: 10-0136A9FE-22561-960.jpg	10/10/2012 05:58:00 PM
<input checked="" type="checkbox"/>			Image file "JPG"	 Newset	Name: 10-589DE5F6-532858-960.jpg	02/01/2013 02:36:00 PM
<input checked="" type="checkbox"/>			Image file "JPG"	 Newset	Name: 10-409CA67A-740665-960.jpg	02/05/2013 10:05:00 AM
<input checked="" type="checkbox"/>			Image file "JPG"	 Newset	Name: sample12.jpg	09/01/2008 05:50:00 PM
<input checked="" type="checkbox"/>			Image file "JPG"	 Newset	Name: 2012-11-01_13-28-20.jpg	11/01/2012 01:28:00 PM
<input checked="" type="checkbox"/>			Image file "JPG"	 Newset	Name: 10-3A8AE5DF-22561-960.jpg	10/29/2012 02:35:00 PM
<input checked="" type="checkbox"/>			Image file "JPG"	 Newset	Name: IMAG0044.jpg	02/06/2013 08:38:00 AM
<input checked="" type="checkbox"/>			Image file "JPG"	 Newset	Name: IMAG0041.jpg	02/05/2013 07:52:00 PM
<input checked="" type="checkbox"/>			Image file "JPG"	 Newset	Name: 10-3B9DC693-532858-960.jpg	02/01/2013 02:36:00 PM
<input checked="" type="checkbox"/>			Image file "JPG"	 Newset	Name: sample05.jpg	09/01/2008 05:50:00 PM
<input checked="" type="checkbox"/>			Image file "JPG"	 Newset	Name: sample08.jpg	09/01/2008 05:50:00 PM

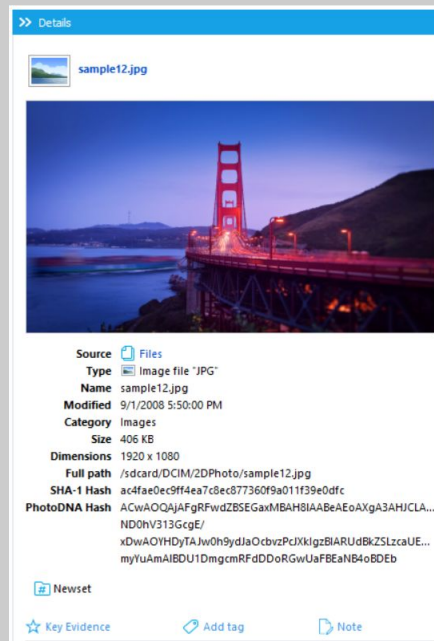


Column 3

Where: On the right-hand side of the Search section.

Uses: This is your details pane.

- Here, information will be unique to the search result that you have selected on the grid (Column 2).
- On the bottom of this pane you will see the option to add the selected item as key evidence, add a tag, or a note.



Oxygen Forensics
901 N. Pitt St, Suite 100
Alexandria, VA 22314
United States
+1 (877) 9-OXYGEN
+1 (877) 969-9436
+1 (703) 888-2327