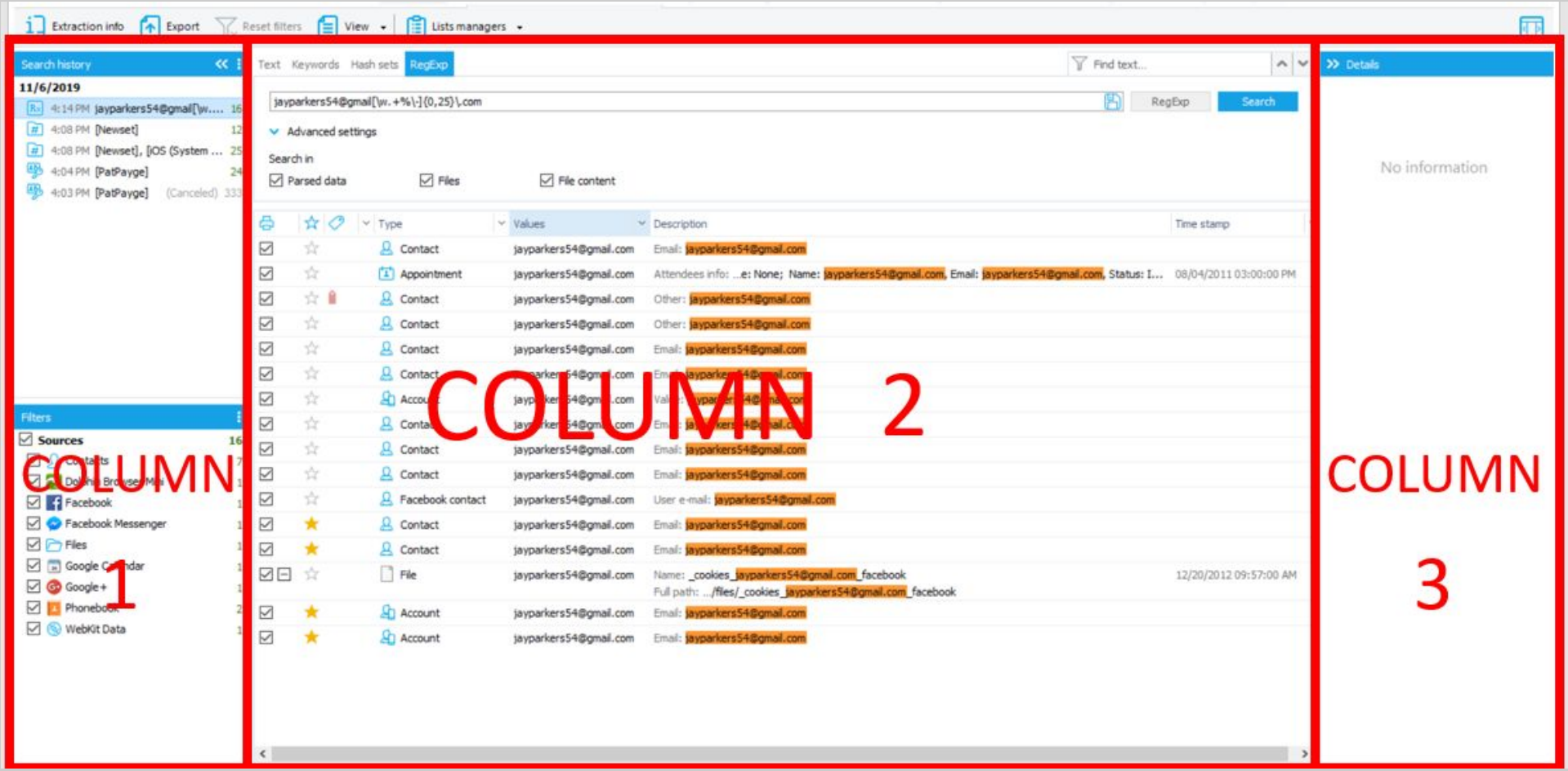
Search

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.

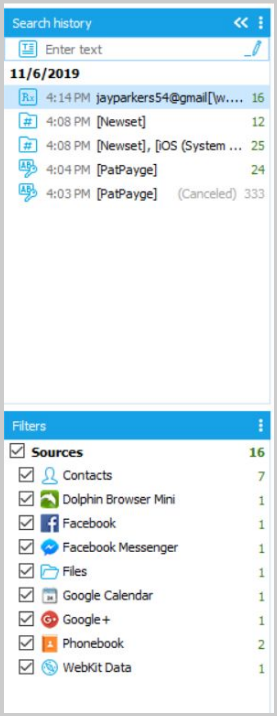
All sections and analytics are laid out in a 3 column fashion across the board making it easier to find the information you are seeking. This document will walk you through which information will be found in each column.



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.

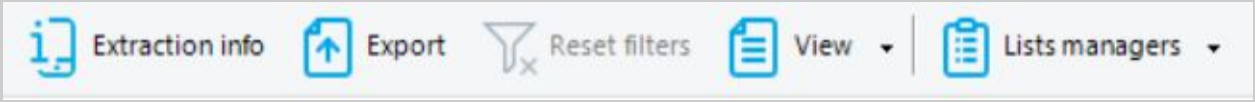
In the upper section of Column 1 you will find all of your search queries along with the number of results yielded.

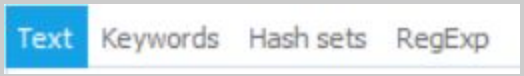


In the lower section of Column 1 you will see all of the sources from which your search results were pulled from.

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:

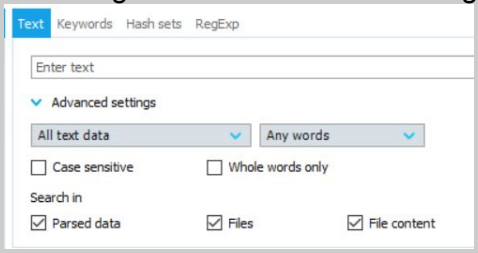
- To move back to the device information click on the box “Extraction info”
- At the top of the screen is the “Export” function. Here is where you can form a selective report on the Search section. You will have the following formats to export your report to: PDF, XLSX, XML, HTML
- To clear out your 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.

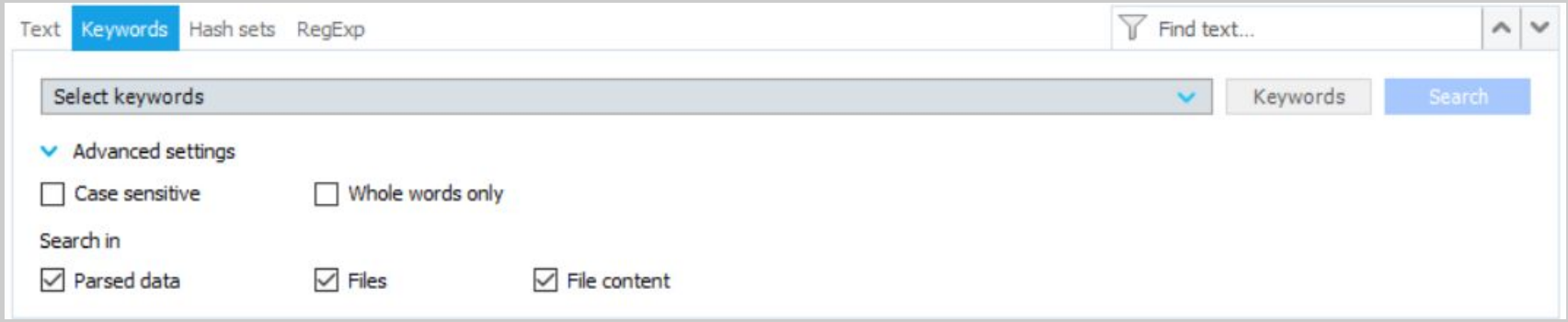
Once you are in the grid inside the section: 

- 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.

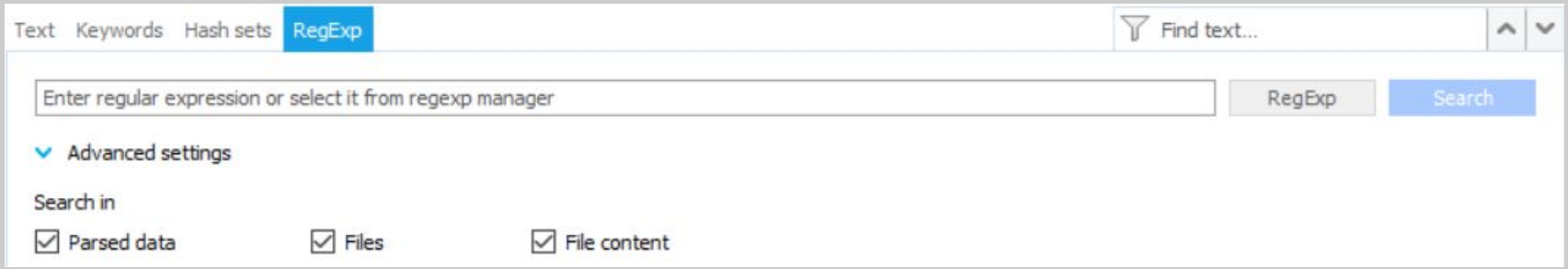


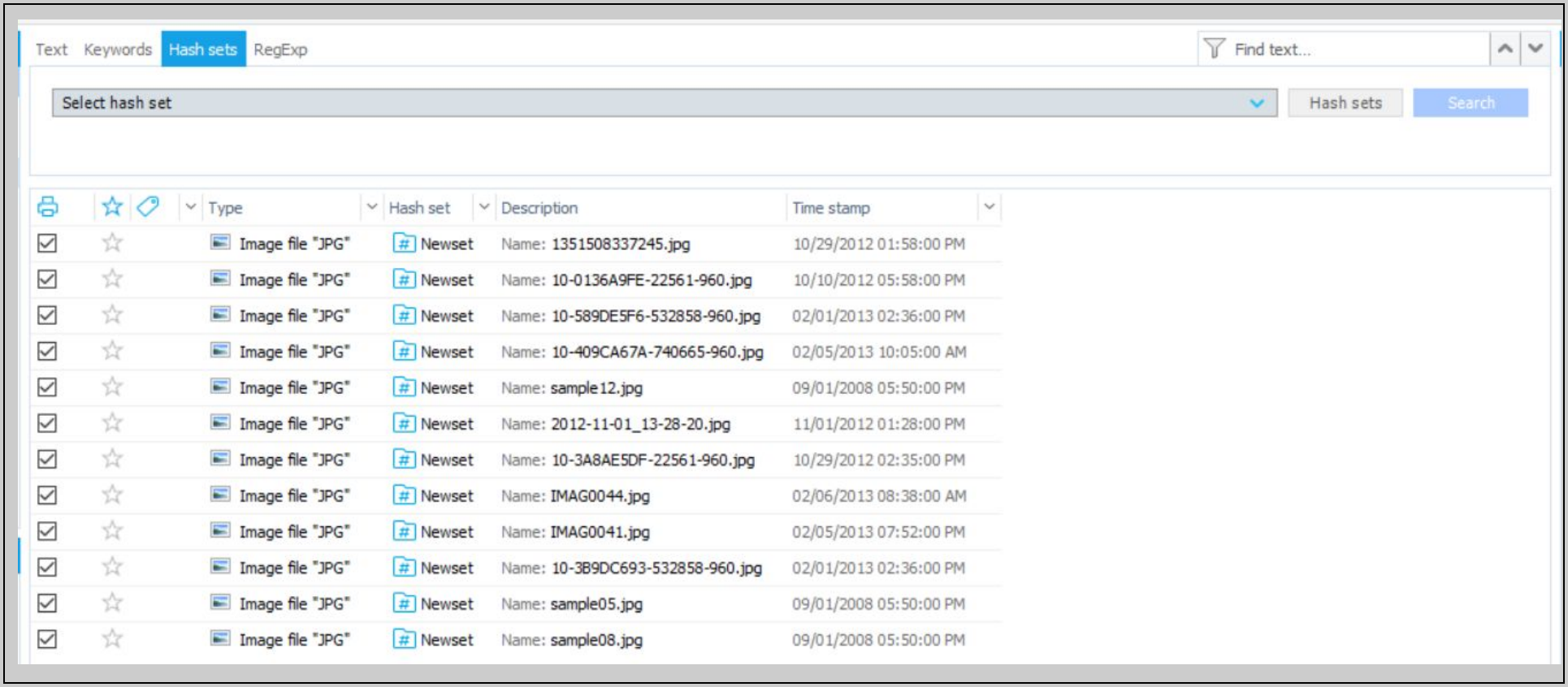
Searching Keywords: Search any Keyword List that Detective already has on file, one that you've created, or imported.



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

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




Text
Keywords
Hash sets
RegExp
Find text...
Select hash set
Hash sets
Search
Type
Hash set
Description
Time stamp
Image file "JPG" Newset Name: 1351508337245.jpg 10/29/2012 01:58:00 PM
Image file "JPG" Newset Name: 10-0136A9FE-22561-960.jpg 10/10/2012 05:58:00 PM
Image file "JPG" Newset Name: 10-589DE5F6-532858-960.jpg 02/01/2013 02:36:00 PM
Image file "JPG" Newset Name: 10-409CA67A-740665-960.jpg 02/05/2013 10:05:00 AM
Image file "JPG" Newset Name: sample12.jpg 09/01/2008 05:50:00 PM
Image file "JPG" Newset Name: 2012-11-01_13-28-20.jpg 11/01/2012 01:28:00 PM
Image file "JPG" Newset Name: 10-3A8AE5DF-22561-960.jpg 10/29/2012 02:35:00 PM
Image file "JPG" Newset Name: IMAG0044.jpg 02/06/2013 08:38:00 AM
Image file "JPG" Newset Name: IMAG0041.jpg 02/05/2013 07:52:00 PM
Image file "JPG" Newset Name: 10-3B9DC693-532858-960.jpg 02/01/2013 02:36:00 PM
Image file "JPG" Newset Name: sample05.jpg 09/01/2008 05:50:00 PM
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