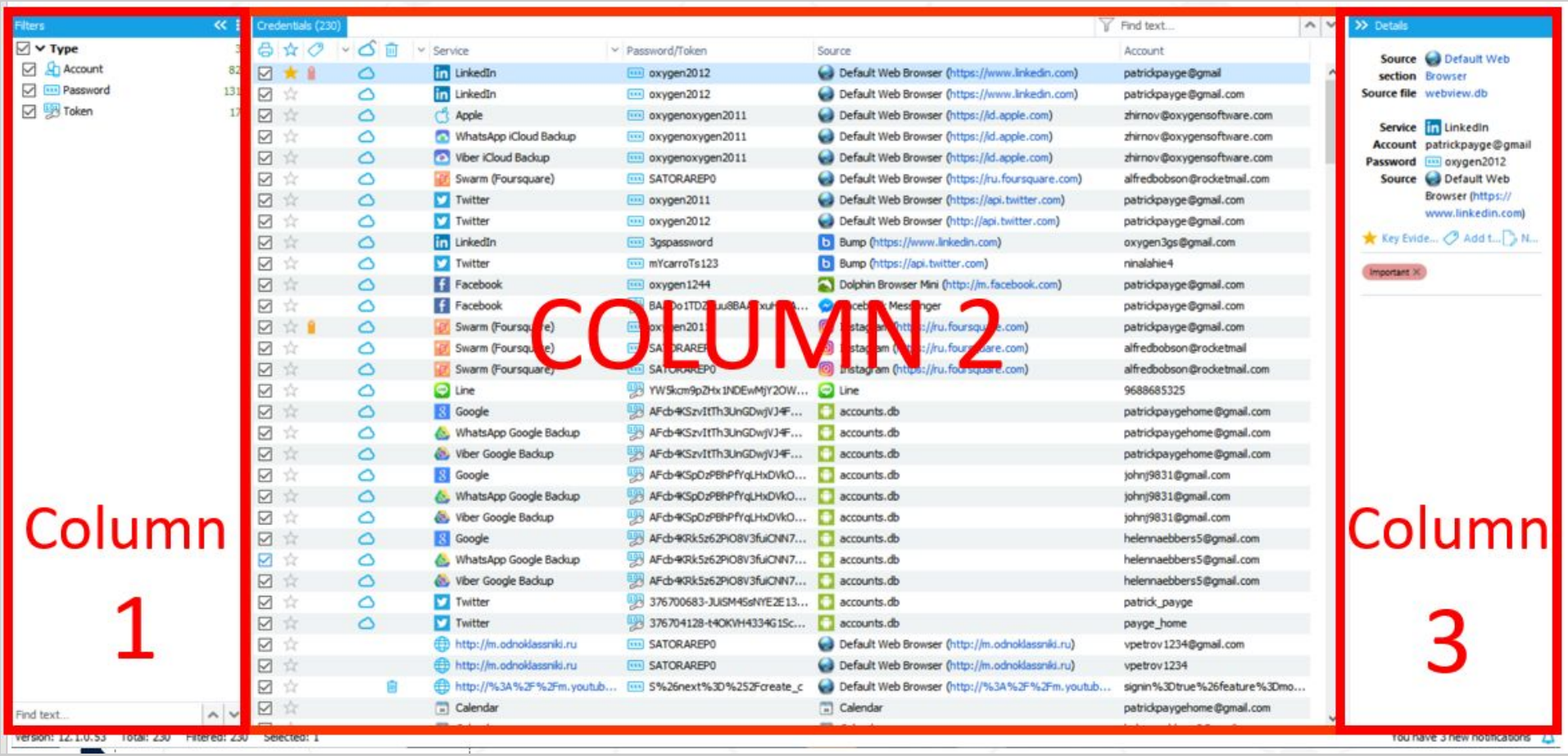
Accounts and Passwords

Getting Started with Detective

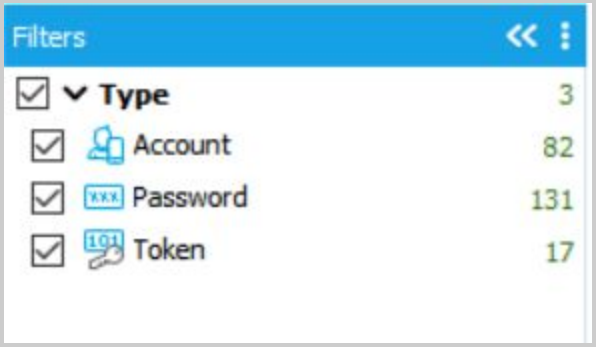
The Accounts and Passwords section displays logins, passwords and tokens extracted mobile devices. The program decrypts credentials from the iOS keychain and Android KeyStore, finds them in application databases and web forms. Investigators can find passwords and tokens to various applications.

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

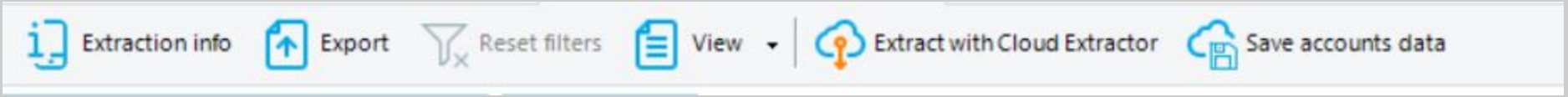
Where: On the left-hand side of the Accounts and Passwords section
Uses: This is a filter where you can narrow your content by selection or deselection. Within this column you can choose what is to be viewed in Column 2 by unchecking or checking the boxes.



In the lower section of Column 1 you will find a “Find text…” box. This is a quick filter box. Once you start typing in the word or name you are searching for it will automatically highlight the matching characters in the column.

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 bar above column 2:

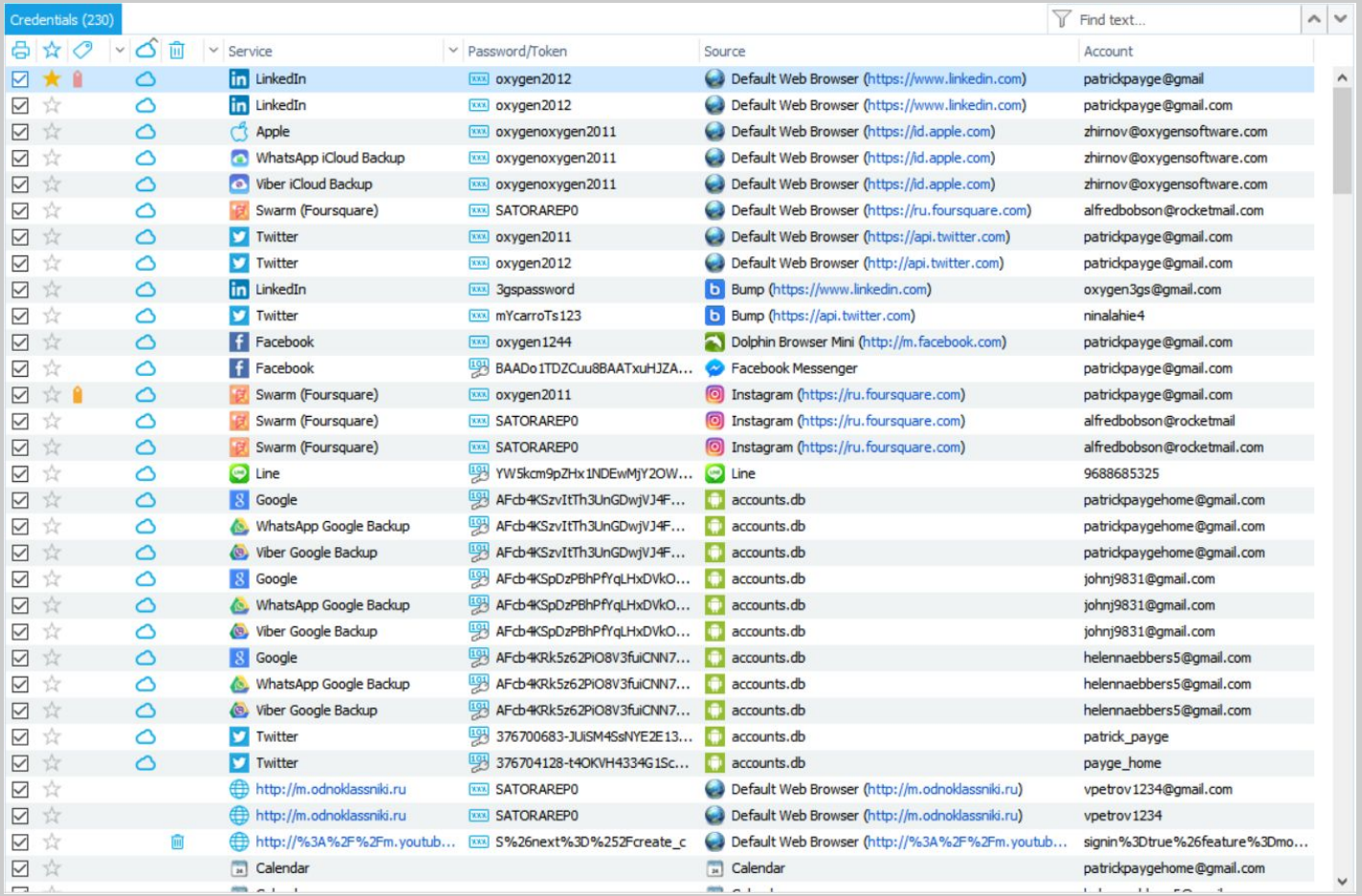
- To move back to the device information click on the box “Extraction info”
- At the top of the screen is the “Export” function. Here is where you can form a selective report on the Accounts and Passwords section. You will have the following formats to export your report to: PDF, XLSX, XML, HTML
- To 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 displayed.
- If the “Maps” button is blue this is an indication that there are geo-locations in this section that can be viewed on OxyMaps.
- Extract with Cloud Extractor: Accounts with a token or password can be extracted with Oxygen’s Cloud Extractor. You will see a blue cloud icon next to the account on the grid if you have the credentials necessary to complete the extraction. Clicking this button will allow you to enter into the extraction process with all credentials already populated for you. See the PDF on CLoud Extractor for more information..
- Save Accounts Data: Here is where you can save your accounts’ information along with the credentials to later import into the Cloud Extractor. See the PDF on Cloud Extractor for more information.

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 grig. If you press enter, your filtered content will be all that is displayed in the grid.

Once you are in the grid inside the Accounts and Passwords 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. If it’s greyed out, it has not been marked as key evidence.
- 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 tags show up. If you choose the box “Tags” 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.

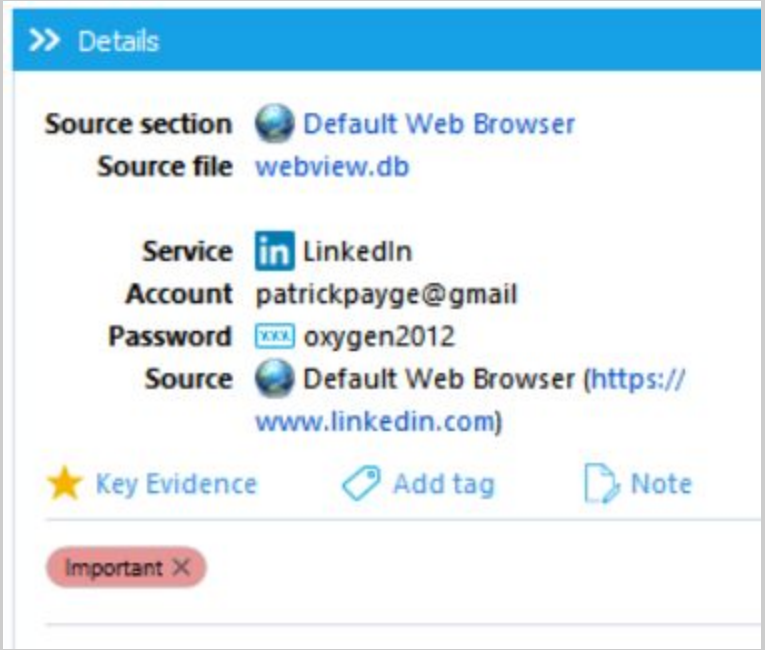
- The Cloud icon: When the cloud icon is present, this represents that the account has a password or token that can be used to access the associated cloud account. You can arrange these in ascending or descending order.
- The garbage can icon: This represents deleted data that was recovered by Detective. You can arrange these in ascending or descending order.
- Service: The name of the application. You can arrange these in ascending or descending order.
- Password/Token: If a password or token is present this is where you will find it. You can arrange these in ascending or descending order.
- Source: The database inside of the device that this information is being pulled from. You can arrange these in ascending or descending order.
- Account: The account name associated with this application. You can arrange these in ascending or descending order.



Column 3

Where: On the right-hand side of the Accounts and Passwords section.
Uses:This is your details pane.

- Here, information will be unique to the call 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