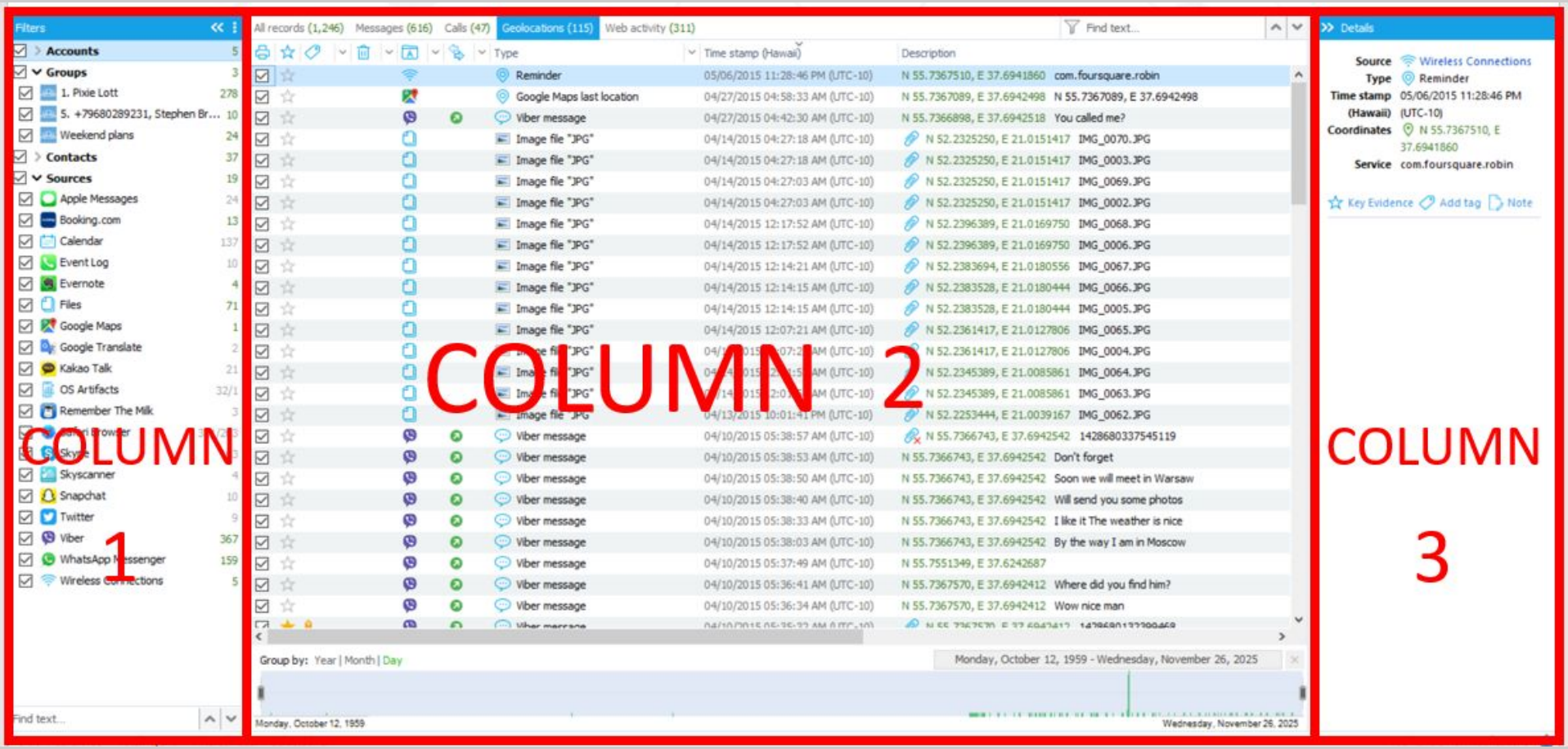
Timeline

Getting Started with Detective

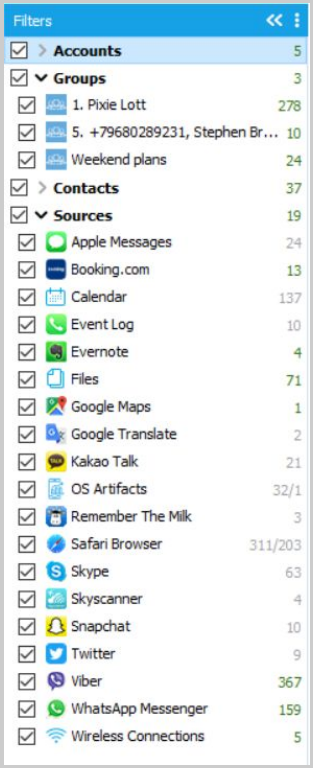
The Timeline section summarizes all events in chronological order: calendar events, messages, calls, web cache, web connections, voicemails, photos and videos history, etc. The section offers investigators a number of powerful filters and convenient data presentation modes that allow them to concentrate on the analysis of the pertinent data only.

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 Timeline 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 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

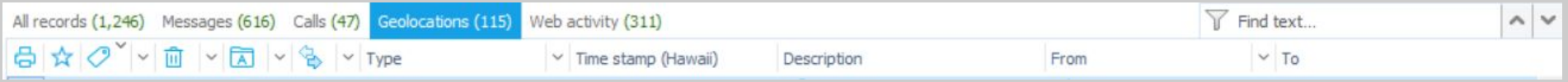
Where: In the center of the section.
Uses: This is your main grid column. Here is where you will see all the content that you have filtered down to on display.

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 Timeline section. You will have the following formats to export your report to: PDF, XLSX, XML, HTML
- To clear out your filters there is a “Reset Filters” button at the top of your screen above Column 2. If the “Reset 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 tag labels 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.

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 Social Graph:

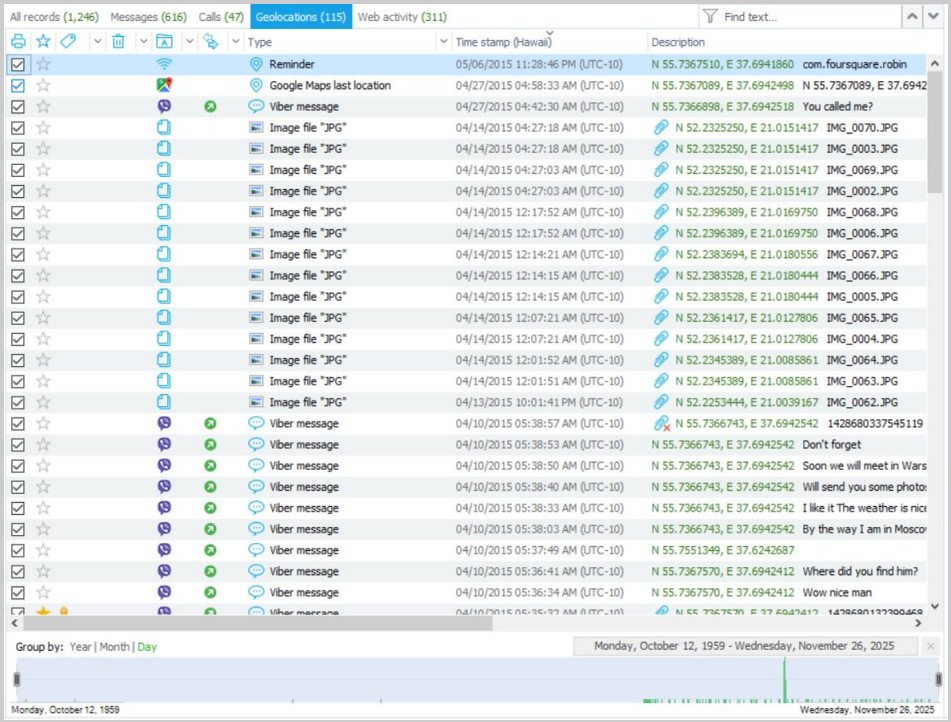


- Data options to display (green numbers beside them indicate the number of files in that category)
  - All Data
  - Messages
  - Calls
  - Geolocations
  - Web Activity
- The printer icon: Here is where you can select or deselect items to be included in your report.
- The star icon: This is a location to add items as key evidence. If the star is highlighted yellow, your item has been marked.

- 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 garbage can icon indicates files that were deleted but recovered by Detective.
- The folder icon: Here you can filter by source. Meaning, if you only want to see events that took place within the Whatsapp application, then you could filter to just that application’s events. All icons under the folder are native to the specific application that the event originated from. You can also arrange the types of applications in an ascending or descending order here.
- The arrow icon: Green arrows indicate an outgoing event, yellow arrows indicate an incoming event, and red arrows indicate a missed event. This is also a filtering dropdown menu where you can filter to which events (incoming, outgoing, missed, failed) you want displayed in the grid. You can also arrange the direction of events in an ascending or descending order here.

The bottom of the grid:

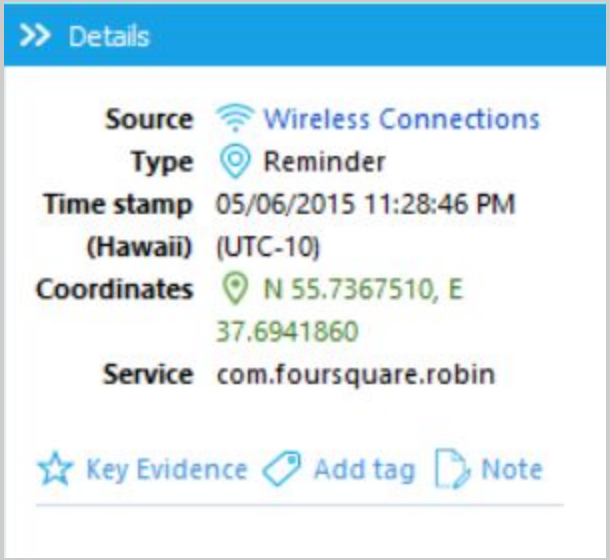
- Here you will find a time filter where you can either use the slidebar or the calendar to filter to the date range you wish to select.
- You can change the view by either looking at the month, day, or hour.



Column 3

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

- Here, information will be unique to the event 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