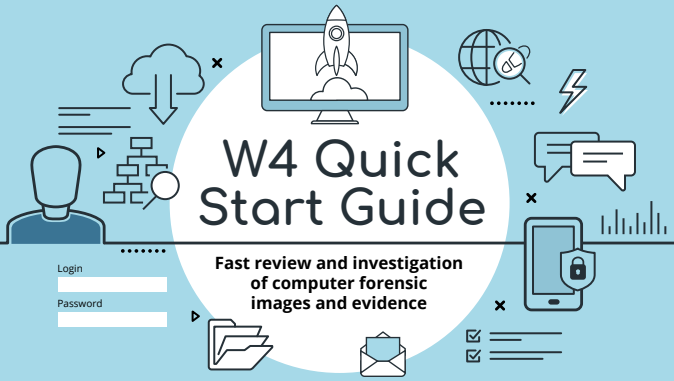
Who | What | Where | When. Simple.

Vound



W4 Quick Start Guide

Fast review and investigation of computer forensic images and evidence

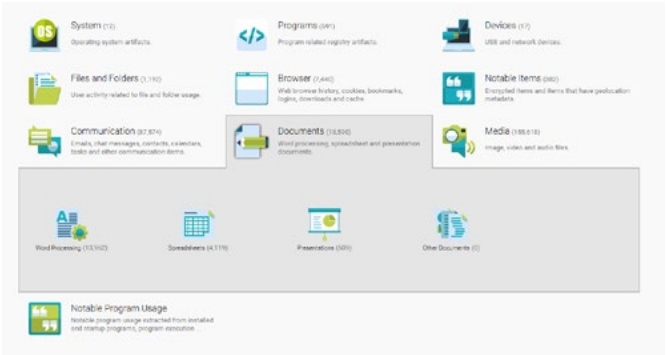
The W4 Interface & Features

Once you have created a case, added evidence to it, and indexed it, the case is ready for review, and the complete dataset can be searched. In this guide we will look at the user interface for W4, and the features W4 has to offer.

1. We have already covered the Sources tab, adding an evidence source, and adding and configuring a keyword list in the previous guide. The last option in the Sources tab that we have not covered is the 'Re-index all sources' button at the bottom of the page. This can be used if the indexing settings need to be changed. Once the indexing settings have been changed, the sources can be re re-indexed so that a new index for the case is created.

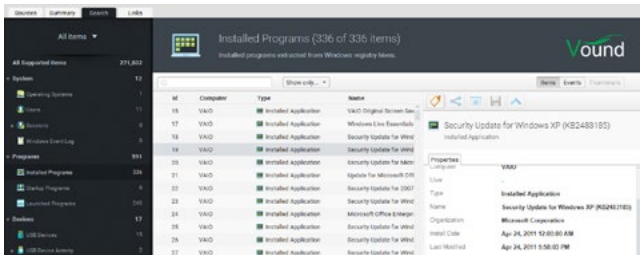
2. The Summary tab provides a summary of the items in the case. The indexed data is divided into several top level categories. These categories include user accounts, system information, devices which have been attached to the system, documents, mail etc.

   When the user clicks on a category, the category is opened so that the user can see the sub categories. The sub categories also show the number of items within those sub categories. Clicking on a sub category will switch you to the Search tab. The items within the sub category will be shown in the table of the Search tab.

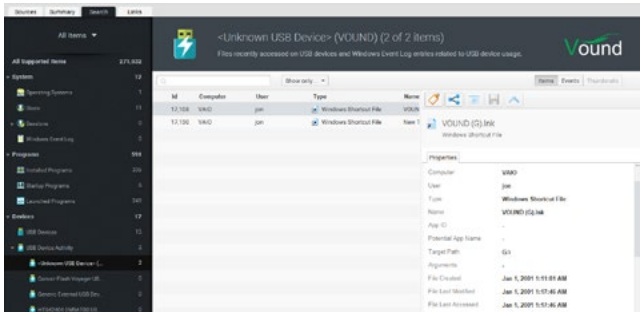


   The bottom part of the Summary tab shows some entries for recent activity on the system in relation to user activity, USB activity and browser activity.

3. The Search tab is where searches can be run and items can be reviewed and analysed.

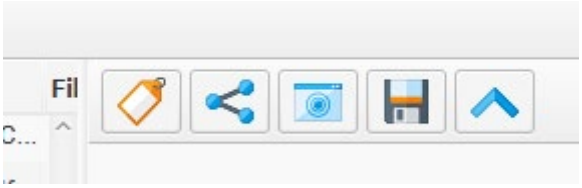


   The Search tab is laid out with a list of facets on the left hand side. These facets show categories of items which the user can select for review. The selection is shown as a list in the centre panel. When an item in the list is selected, the properties for that item are shown in the right hand panel.

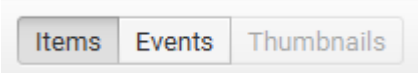


4. when reviewing an item, the right hand panel has a number of useful controls and options. Depending on the file type, several tabs containing information and/or views of the item will be shown. For example, some items may only show the Properties tab, whereas a Word document will also show a Preview tab. There may also be an Attachment tab shown if the document has embedded items.

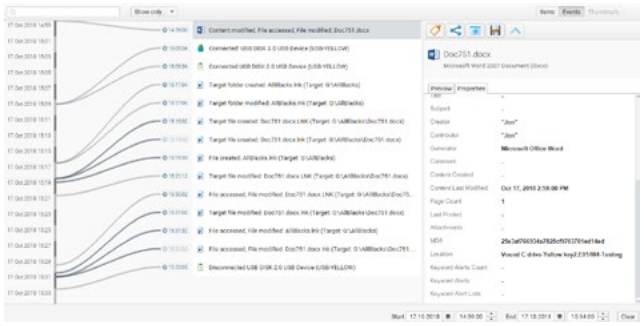
   At the top of the panel are buttons to tag the item, to open the item in its native application, to export the item, and to add the item to the Links graph which can be seen in the links tab on the left hand panel.



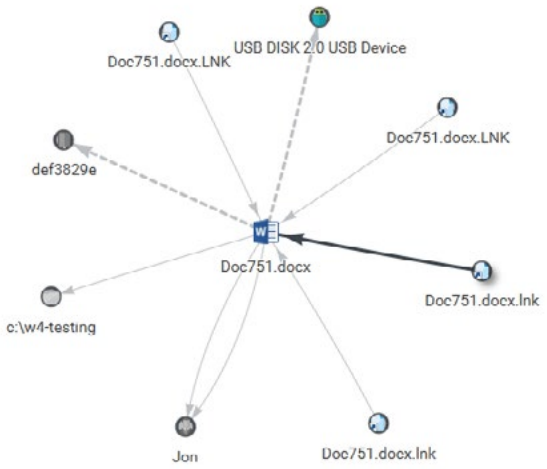
   We will get to the Links tab soon, but above these buttons are additional buttons to change the view of the items in the centre panel. By default the Items option is enabled, which lists the document etc in a table view. The Thumbnails button will show thumbnails of images. This button will be disabled if there are no images in the table, or if there are images mixed with other file types in the table (e.g. when the user selects the documents and images categories).



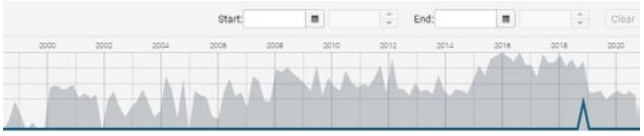
5. The Events option shows the list of items in a timeline type view. This is useful if you are investigating something like USB device activity and file access on a system. You can set which categories to include, and set the time frame for the activity. In this example, W4 has done all of the hard work in the background, and is showing you a chronological list of events for file and USB activity that occurred on that system, within that time frame.



6. As mentioned above, an item can be shown in the Links graph. The is done by highlighting the item, then clicking on the 'Add to links graph' button. W4 will then switch to the Links tab where you can see the links for the selected item. Using the example with the USB device and file activity above, we can view the relationships between these items. In this image we can see that the document has links to the C: drive of the system, and also to a USB device. Further analysis would show that the file originated on the C: drive, then the file was created on the USB drive, which indicates that the file was copied there.

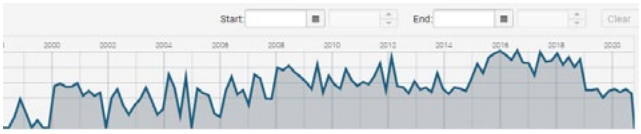


7. We also show a timeline below the centre and right hand panels. The grey shaded area of the timeline shows all of the items in the case based on dates. This is useful for quickly identifying gaps in the dataset.



   The solid line at the bottom shows the timeline for

the list of items that you have selected, and are shown in the centre panel. If all items in the case are selected then the solid line will follow the grey shaded area.



A specific time frame can be set by adding start and end dates in the fields provided. You can also click in the timeline itself, and drag your mouse to highlight a custom section of the timeline. Note that only items in that date range will be visible. The Clear button on the right will clear any date selections that have been made in the timeline.

When in the Events view, the timeline may show an orange shaded area with a solid orange line. This shaded area represents the visible items which are shown in the Events view. This shaded area will move along the timeline axis when you are scrolling through the items in the Events view. The solid line represents the item that you have your move over at the time. This line will move when you hover over other items with different dates.