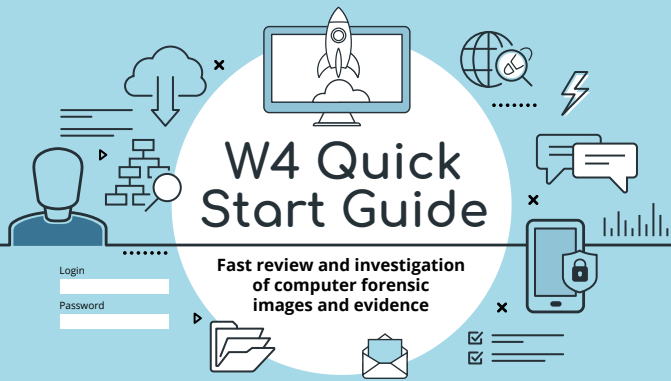




Who | What | Where | When. Simple.

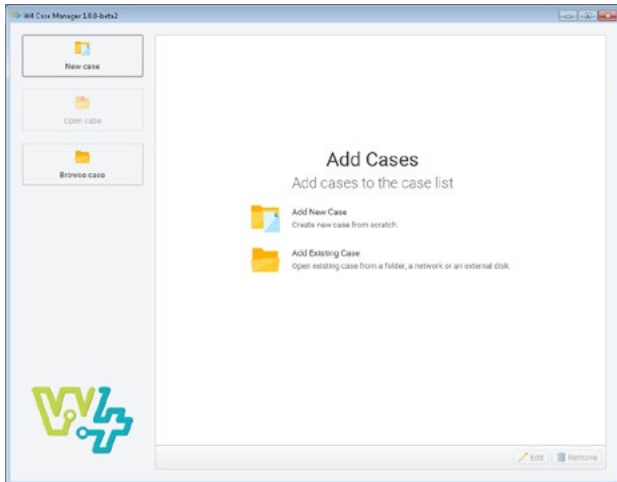


W4 Quick Start Guide

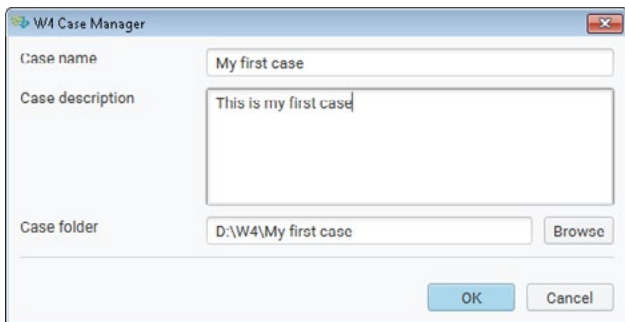
Fast review and investigation of computer forensic images and evidence

Creating Your First Case

1. Once W4 has been installed, start the application by double clicking on the desktop icon. W4 will show the Case Manager. This is where you can conduct different tasks such as opening an existing case, adding a case that has already been created, and creating a new case.

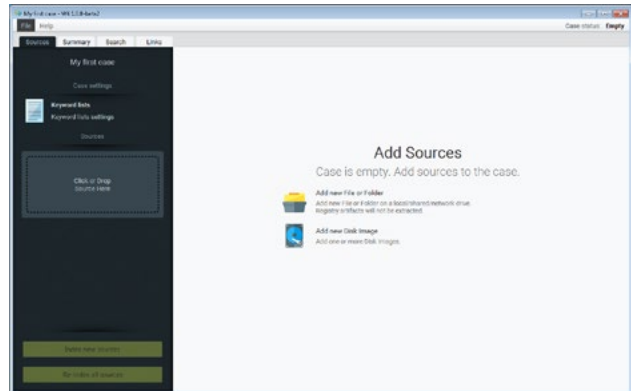


2. Click on the New case button at the top right, or the Add new case option in the centre of the screen. A window will be shown where you can type a name for the case, add a description (optional), and path to the folder where you want the case to be created.



3. Once the details for the case have been entered, the new W4 case will be opened in the Sources tab. This

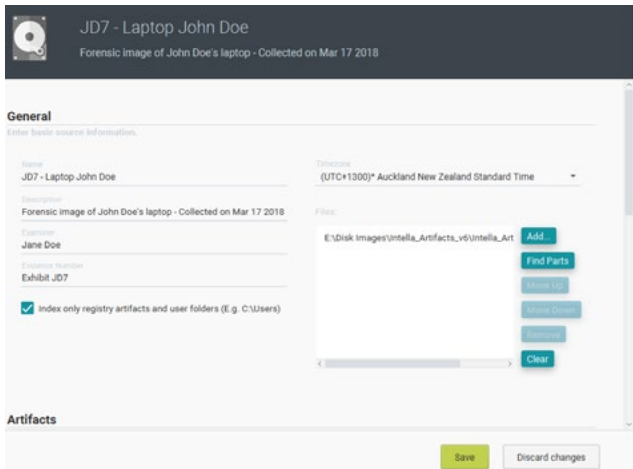
screen allows you to add evidence (folders containing files or disk images) to the case. You can drop the evidence on the target area shown in the left side panel. Or, you can click on one of the options in the centre of the screen, and navigate to the evidence source.



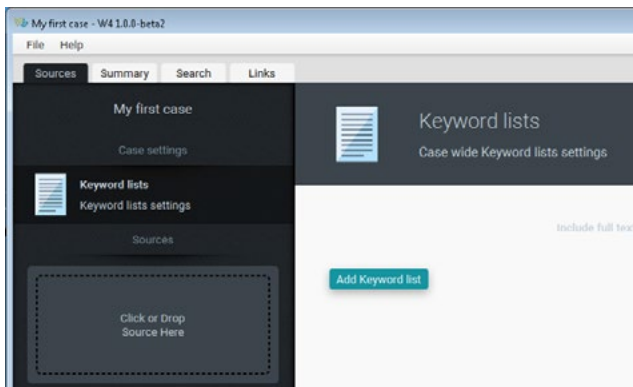
4. Once the evidence has been added to the case, you can add some basic source information, and configure settings for the source.

- General – These settings can be configured:
 - The source name
 - A description
 - The examiner's name
 - An evidence number for the source
 - The time zone for the source
 - An option to index only the registry artefacts and user folders
- Artefacts – Various artefacts located in the source can be enabled, or disabled.
 - Keyword lists – We will cover this below.
 - Advanced settings – These include the follow options:
 - To process embedded images in email and documents
 - To process archives (e.g. Zip, RAR, 7Zip etc)
 - To recover deleted emails and files
 - To index the full email headers

Once the source has been configured, click on the Save button to save the settings.

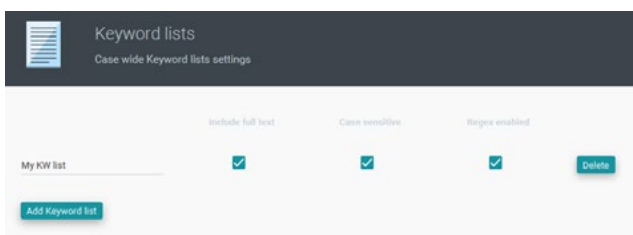


5. This Sources tab also allow the user to add a keyword list prior to indexing the evidence. To add a keyword list, click on the Keyword lists option in the left hand panel, then click on the Add keyword list button in the centre panel. Navigate to your keyword list to add it to the case.

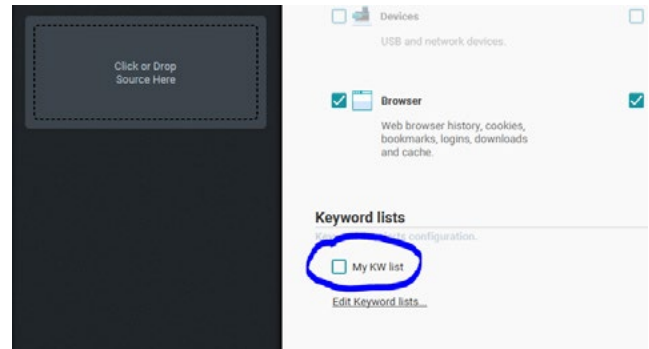


Once the keyword list(s) have been added, you can configure how W4 should use the list for searching.

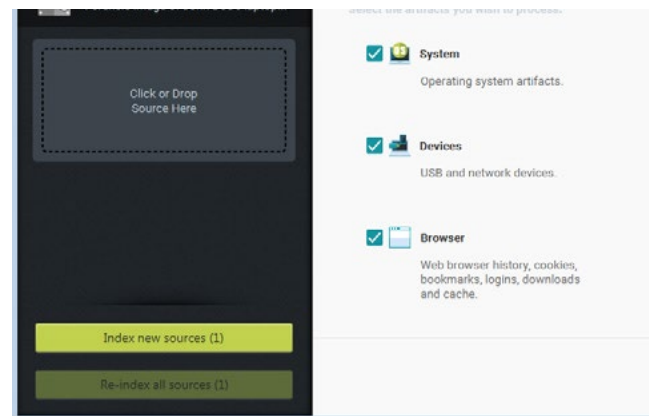
- Include full text: This option will conduct the searches over the full text, instead of just over the metadata.
- Case sensitive: This option treats the search terms as they are entered in the keyword list. This includes matching the case of the characters in the term.
- Regex enabled: This option allows regular expressions in the keyword list.



Once the keyword list(s) are configured, click on the Save button to save the settings. Make sure that you go back onto the source that you added and enable the keyword list so that it will be used during the indexing process.



6. Now that the evidence has been added, and the keyword list has been configured, you can start the indexing process by clicking on the Index new sources button at the bottom of the left hand panel.



7. When the indexing process is running, you can see the progress by clicking on the Summary tab. Artefacts will be populated 'on the fly' while the indexing is taking place. This allows the user to start looking at the processed data before the indexing is complete.

The Summary tab will show a message when the processing is complete. For more information on using W4, see our other guides and documentation.

