The Case Management for CSI Linux

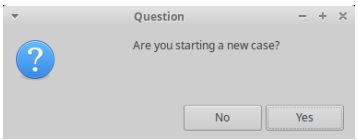
CSI Linux has a lot of custom applications built in including a proprietary case management system built by our developers. This will build the folder structure for each case, dump evidence from selected applications, build a report template, and hash the case data when you close the applications. This helps take the mundane activity out of starting your case and automates some of the basic functions, allowing you to focus on the investigations.

This means you can spend more time focusing on what you need to do rather than building the case backend and making sure your evidence is hashed and archived. Every time you use one of the case related CSI Tools, the case folder will be archived on exit. This provides and extra layer of reliability for your evidence items.

Knowing this, you need to realize that the required disk space will grow for related to the cases you do and the times you exit the case. Consider this when planning for environmental planning and engineering. Consider moving your Cases folder to an external drive.

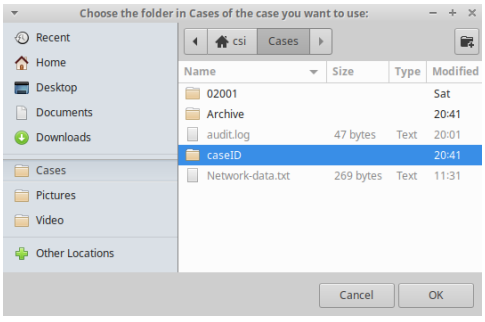
The basics…

Double left click on the "**Start a case**" icon on the desktop, or go to the "**CSI Linux**" icon on the top left, left click the "**CSI Linux Tools and Case Management**" option, and left click on "**Start a case**". This should open up a new window that asks you id you want to start a new case or open an old one.



Opening a preexisting case

1. Left click on "No".
2. Find the folder related to the case you want to continue. Then Left click "**Ok**".

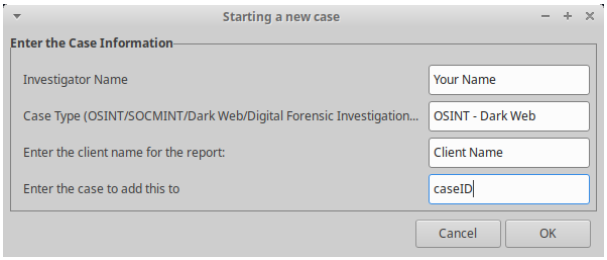


3. Fill in the required information.
4. Left click "**Ok**".

Starting a new case

Test

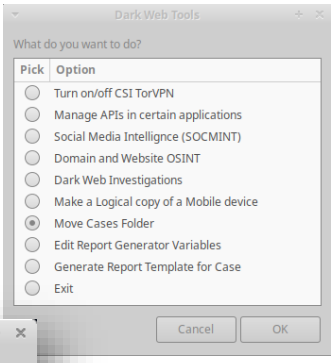
1. Left click on "**Yes**".
2. Fill in the information including Investigator Name, Case Type, Client Name, Case ID, and Left click on "**OK**".



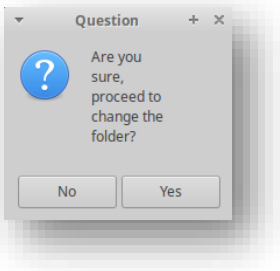
3. This will create the case folder and subfolders in the ~/Cases area.

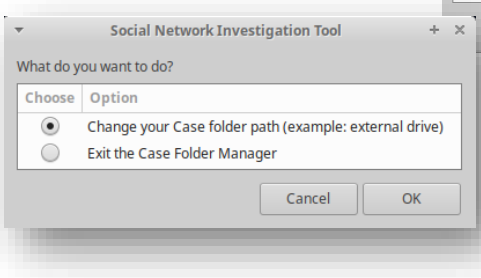
Moving the Case folder to another location

If you need to move your base "**Cases**" folder to another location (network drive or external hard drive), left click on "**Move Cases Folder**" and then left click on "**Ok**".



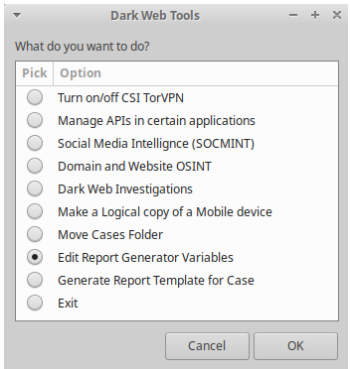
1. Left click on "**Change Your Case Folder**" and Left click on "**Ok**".
2. You will be asked if you are sure if you want to move your base Cases folder. If you are sure, left click on "**Yes**".



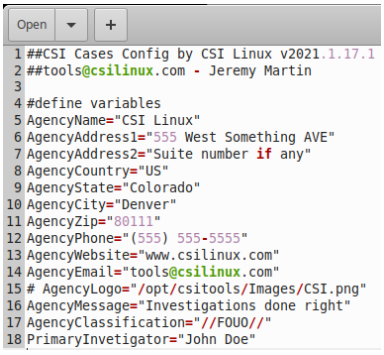


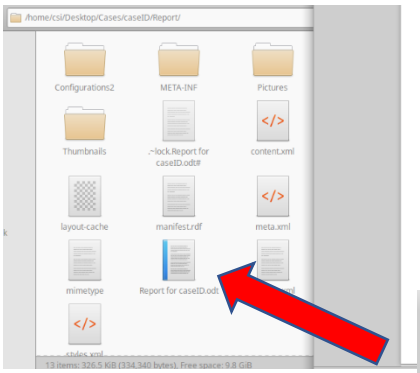
Report Option

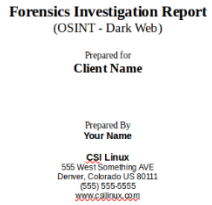
1. You will now be given the option for what you want to do. If you want to create a report template, you need to make sure your configuration file is set correctly. This will include your agency or organization information. Chose "**Edit Report Generator Variables**". Left click "**OK**".

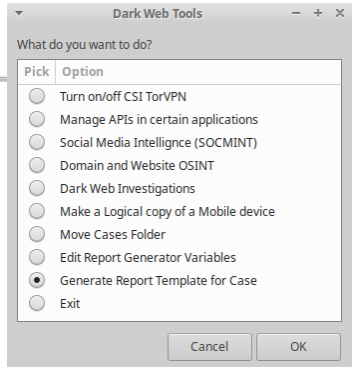


2. Edit the variables as needed, then save an exit the file.



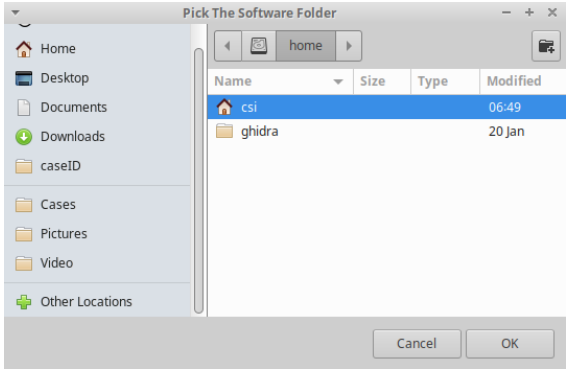






3. Then, left click on "Generate Report "**Template for Case**", then left click on "**OK**". This will generate a report template with the variables that you have previously chosen and you can use and saves it into the: "**/home/csi/Desktop/Cases/caseID/Report/"** folder.
4. Edit the report as needed. The template si the file that ends in a the "**.odt**" extension.

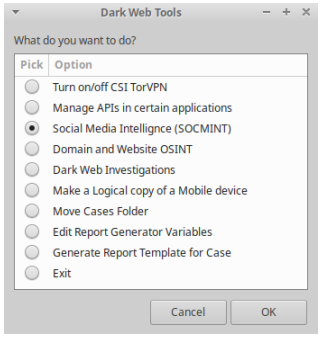
Note: *You can modify your base template for your agency or organization by modifying the file located at "/home/csi/Documents/Templates/csi-template.odt".* Pick the folder, drive, or network share you want to move your cases folder to, then lift click on "**Ok**".



This will create a link from the original locate to the new location, so the rest of the tools that work with the Case Management tools will continue to work.

Without a report

Chose the application that focuses on the type of investigation that you want to run from the list provided.

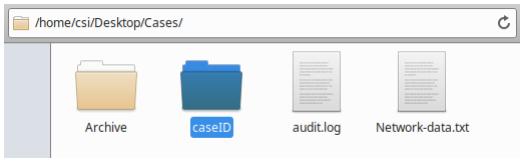


This will add the evidence found using the selected tools into the case identified in the first section.

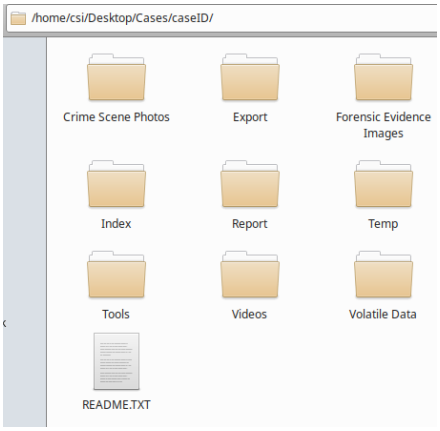
Each time you exit one of the tools selection applications, the case will be closed. This means that the case folder will be cleaned up, the files included will be hashed, and the contents archived as a copy with a timestamp and saved to the "**~/Cases/Archive**" folder. Just be aware that this can start to use a lot of hard drive space over time.

The Case Folder

What happens in the Case Folder? When a case is started, the applications check to see if the case exists. If it does, the contents just get added to the proper sub folders. If it does not, then the folder structure is generated for you. This will include the case name (in this example it is "caseID") and the Archive folder that will contain a backup of your cases.



The directory structure inside the case named folder should look similar to this:



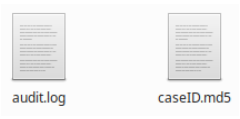
You should add your evidence in the corresponding folders. If you generated a report template, it will be located in the "Report" folder as an .ODT file. You can open that file up with LibreOffice. Most of the tools and applications run through the CSI Linux tools will place their output into the "Export" folder. You can move the results into the proper folders.

If you have forensic images of a drive or evidence items, these should be placed in the "Forensic Evidence Images" folder.

If you are going to use other tools like Autopsy, it is a good idea to put the case data in the Tools folder. This will make sure that all the data from these other tools are tied with the case.

Closing the case

When the case closes, any files that were added or created in the case related folders will be hashed and two files will be created or updated. These are the "audit.log" which contains a chronological record of the investigation activity and the "casename.md5" file that includes an MD5 hash of all files in the folder.



In the base "Cases" folder "\Archive", the case name folder is added to a compressed zip file and also MD5 hashed to retain a more forensically sound evidence storage.