

FTK Crashes or Hangs on Certain Files

If FTK crashes or hangs on a file you can either exclude the file by refining the evidence or by reindexing the case while ignoring the problem file that FTK is crashing or hanging on.

Please note that you will need to reprocess the case when FTK crashes or hangs on a particular file.

Follow the steps below to exclude the file from the case by selecting the Refine Evidence – Advanced option.

1. From the **Add Evidence to Case** screen click on **Add Evidence** and choose the item that you want to add to the case.
2. Click on the **Refine Evidence - Advanced** button and select the **Refine Evidence by File Path** tab.
3. Browse to the directory the problem file resides in.
4. Uncheck the directory so that the problem file will be excluded from the case.

Follow the steps below to ignore the file from the case by creating a KFF Ignorable hash file.

1. Create a file named hash.csv with the following two lines:

```
MD5  
16C3A5060A5D7D2FD6C1D647B40442DC
```

The MD5 can be taken from your case log. If you can't get it from your case log, you can use FTK imager to browse to the problem file, right-click it and choose to write the hash to a file called hash.csv.

2. In FTK, select **Tools**, then **Import KFF Hashes**.
3. Select the hash.csv file you generated.
4. Enter a hash set name, such as "FTK Workaround." Make sure the radio button reads "Ignorable."
5. Click on OK.

Make sure **Extract Files from KFF Ignorable Containers** is unchecked on the Refine Case-Default screen when you reprocess the case.