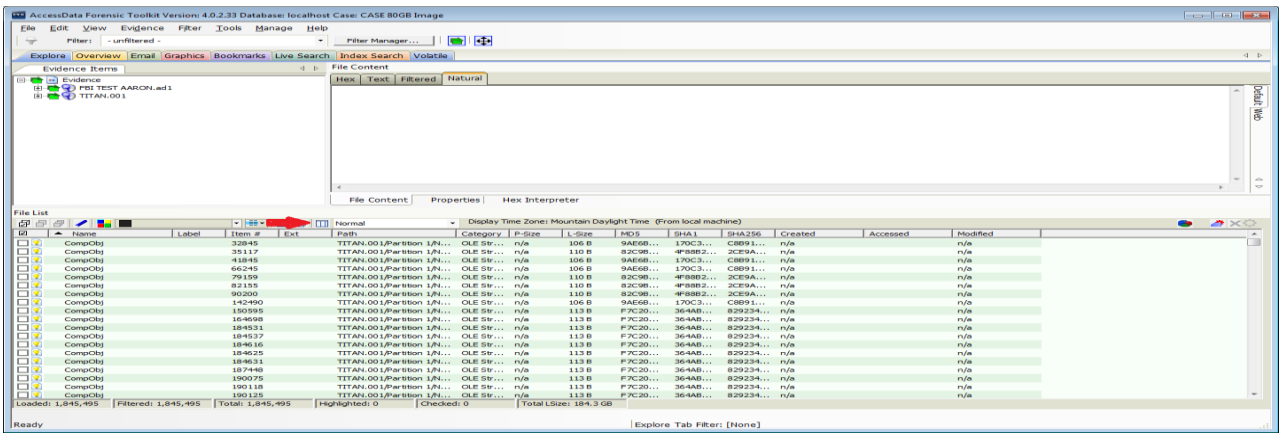
Creating KFF from Bookmarks

1. Change your column settings to only show MD5

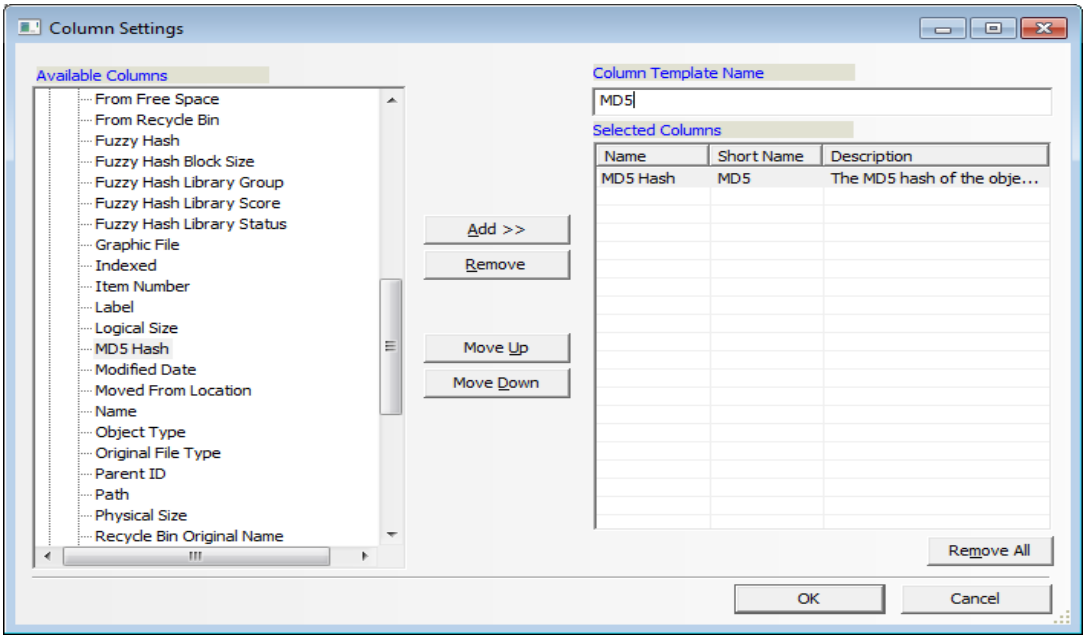
2. Click on the column settings icon in the file list.



3. Select New

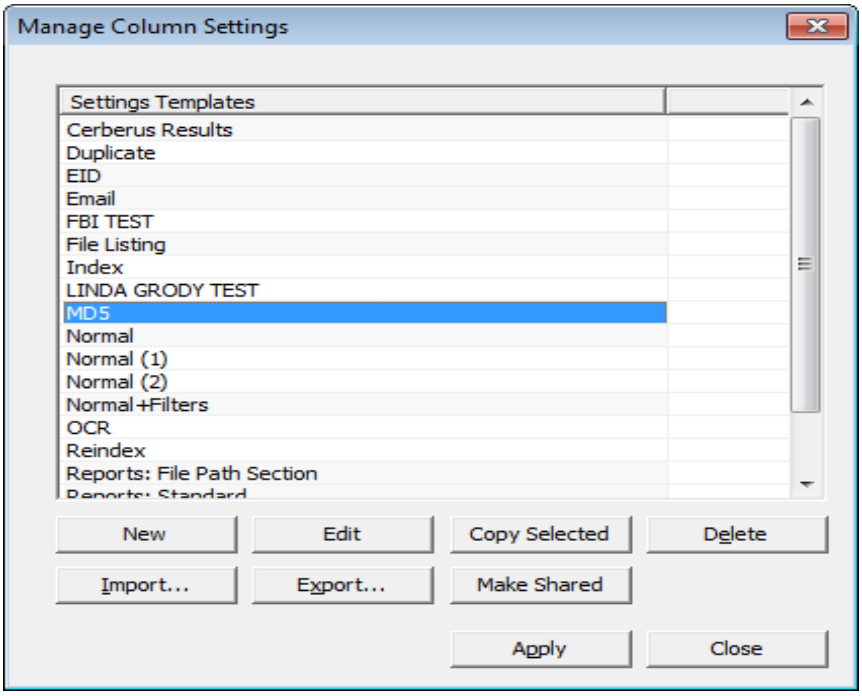
4. Name the Column Template Name MD5.

5. In the available columns expand the Common Feature and Select and Add MD5 hash.



6. Click OK.

7. Select the MD5 Column you just created and click Apply.



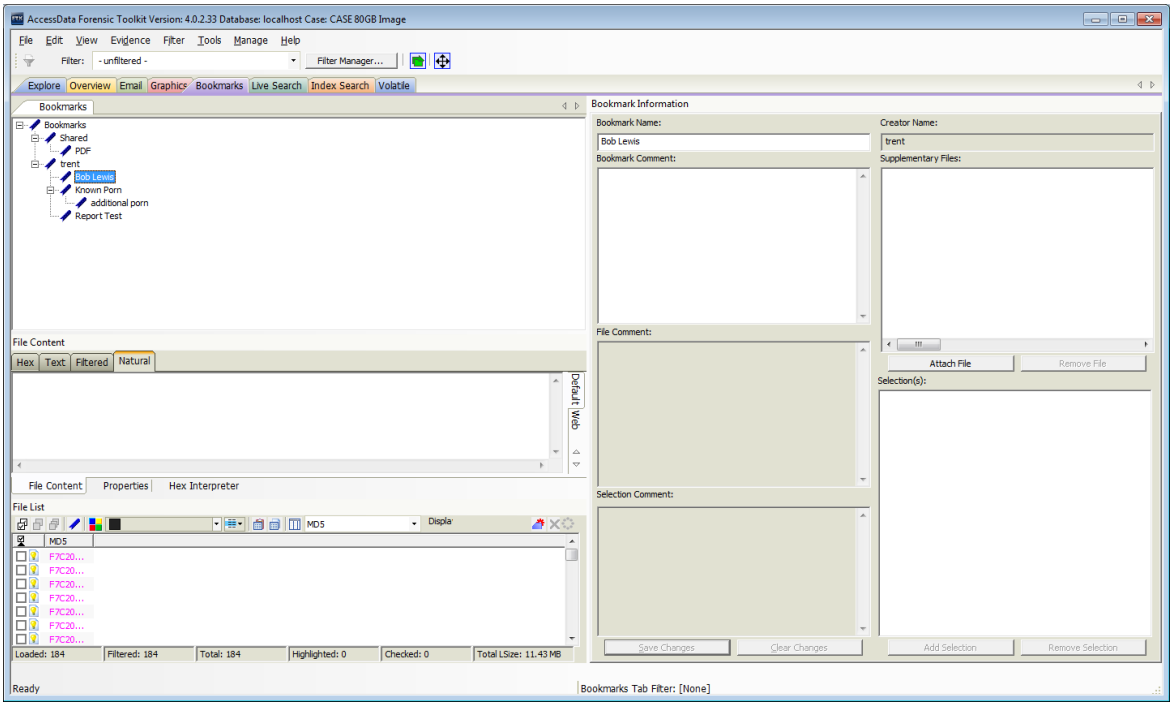
8. Click close.

9. Click on your bookmark tab.

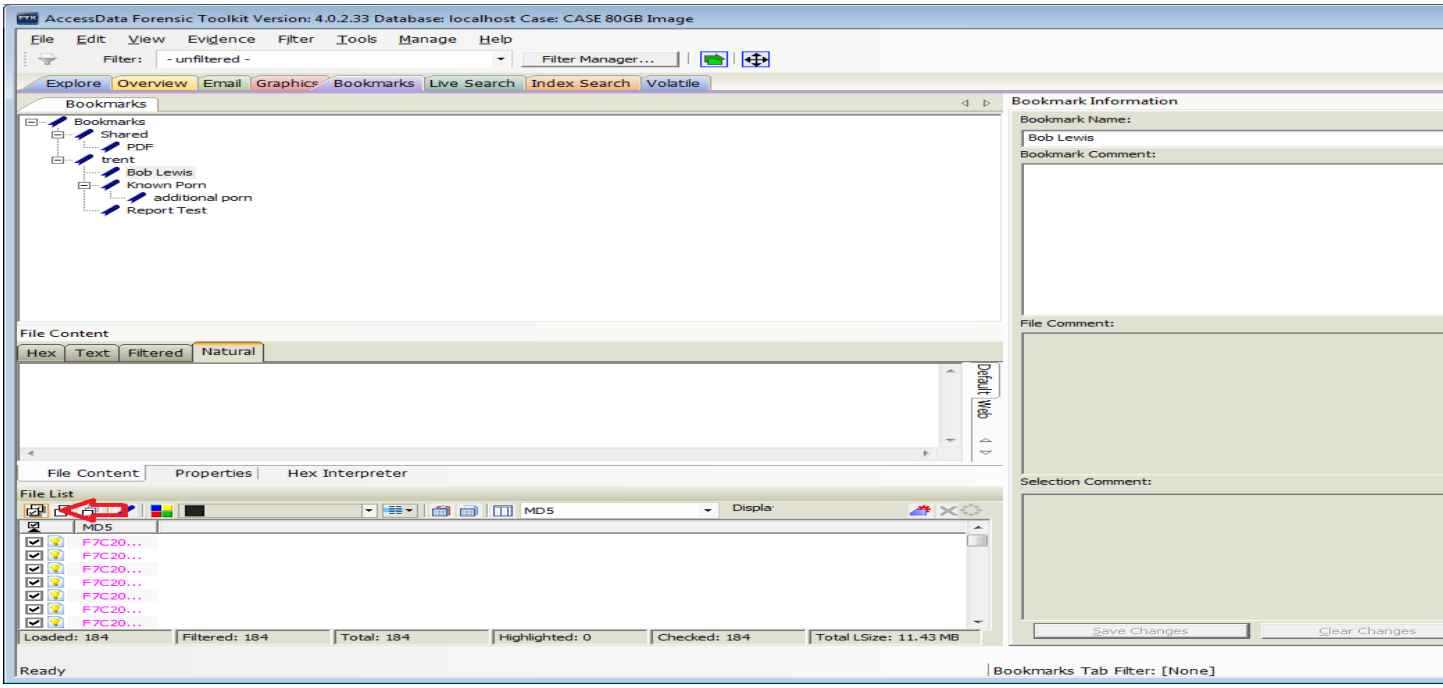
10. Do the following per each bookmark name you have created.

11. Repeat steps 1-8 in the Bookmarks Tab.

12. Select a single bookmark.



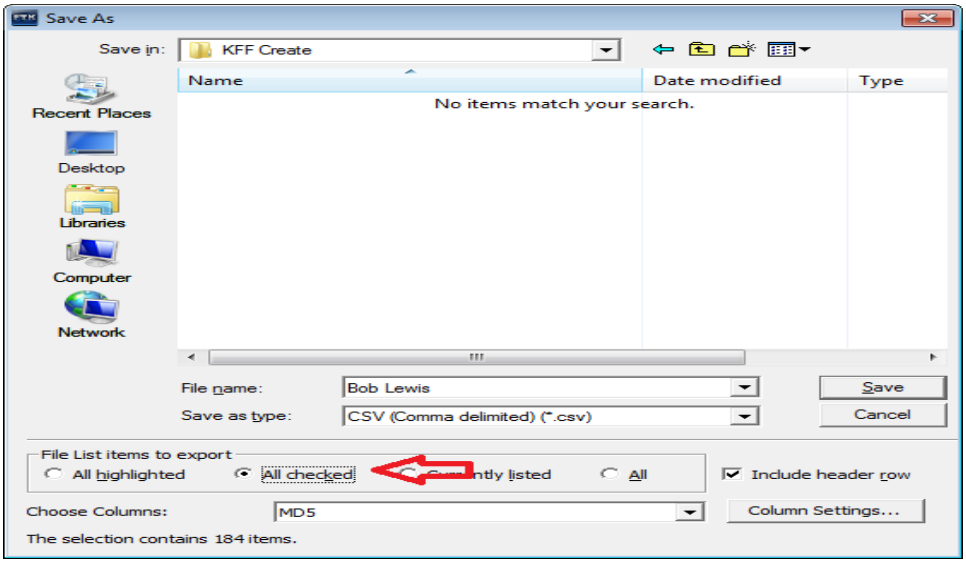
13. Select all in the file list for this bookmark.



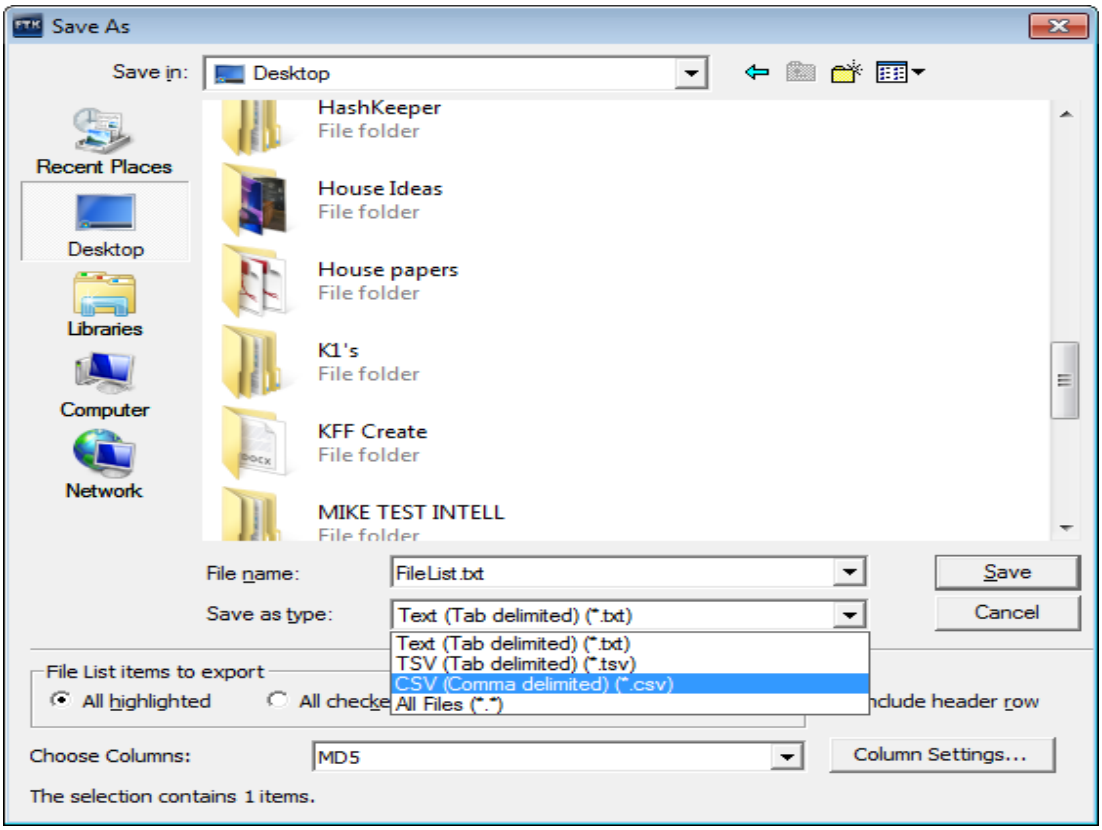
14. Right Click on a file in the file list and select Export File List Info.

15. Name the file the same as the Bookmark name.

16. Make sure to select All Checked in the File List items to Export.

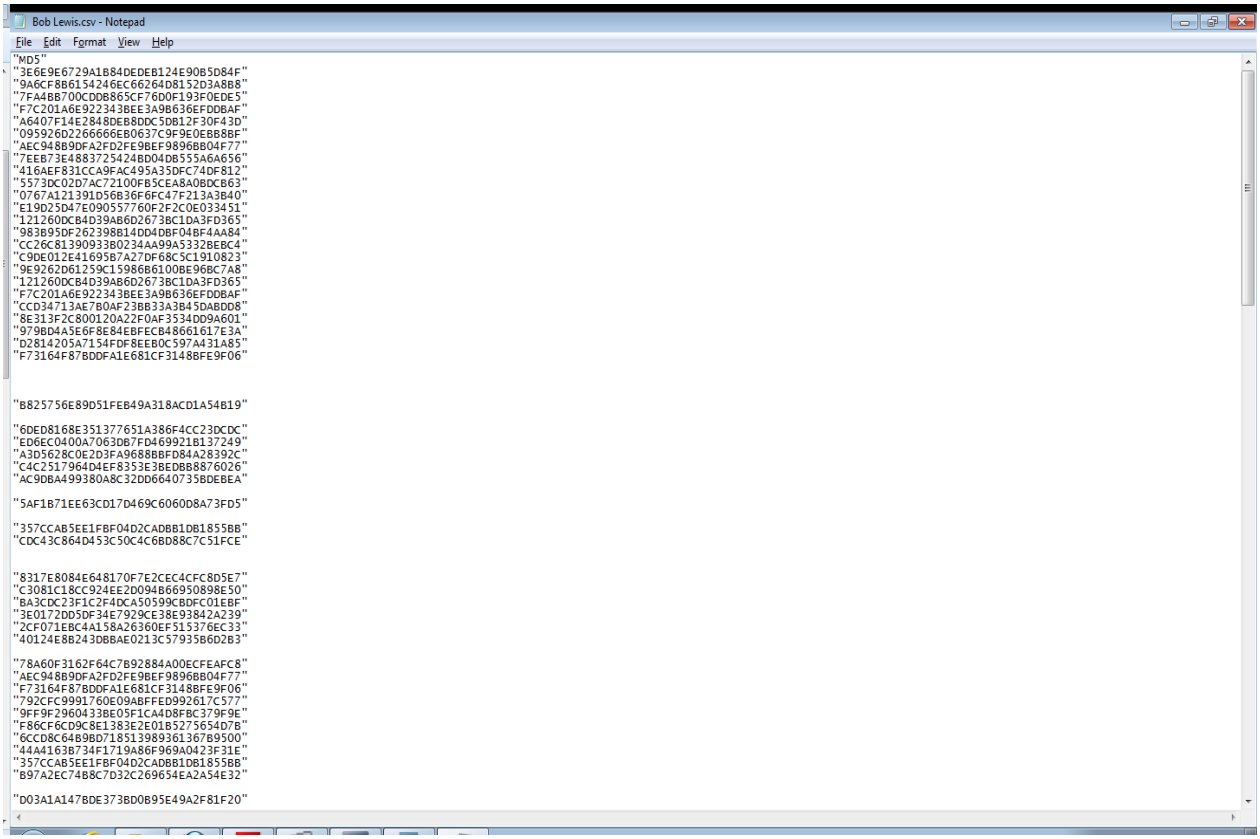


17. Save as a CSV file



18. Click Save.

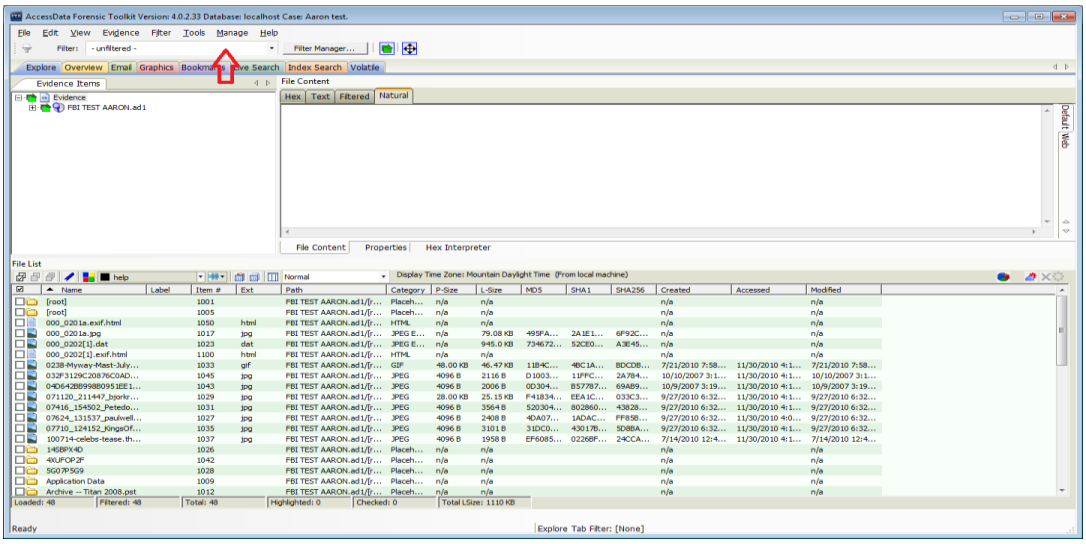
19. Open your csv file that you have created. It will look something like this.



20. Repeat steps 12-19 for all of the bookmarks you wish to create KFF's with.

21. Open the case in which you want to add the custom KFF's.

22. In the case click Manage at the top of the case screen.



23. Click KFF and then Manage.

24. Click Import

25. Click Add File and add your modified CSV file to your path.

26. Click OK.

27. Click Process Files.

28. Click Done when finished.

29. Under the Defined Groups click New.

30. Give a name to the Group Information.

31. Click OK.

32. Under the Defined Groups, now click on the Group Name you just created and then click Edit.

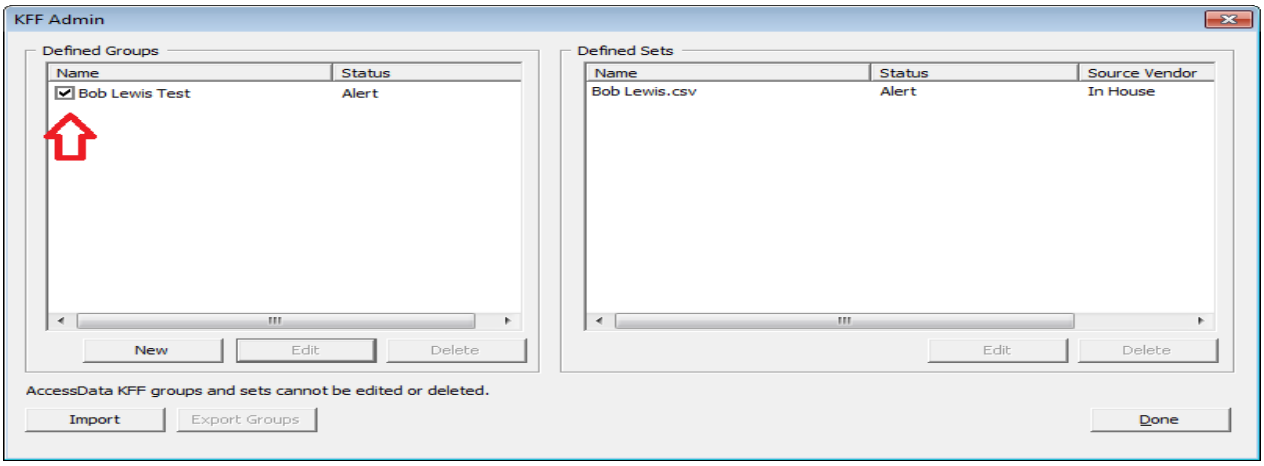
33. Click on the name you created in the available sets and add it to the items in the group.

34. Click OK.

35. Repeat steps 23-28 29-34 for each bookmark CSV file you have added to this case. If you choose you can keep the same Defined Group for all of the defined sets. User preference.

36. Make sure that the defined group status is set to alert. Click on the Group name and then edit to change it if you need.

37. Make sure that you place a check mark in the box next to the Defined Group.

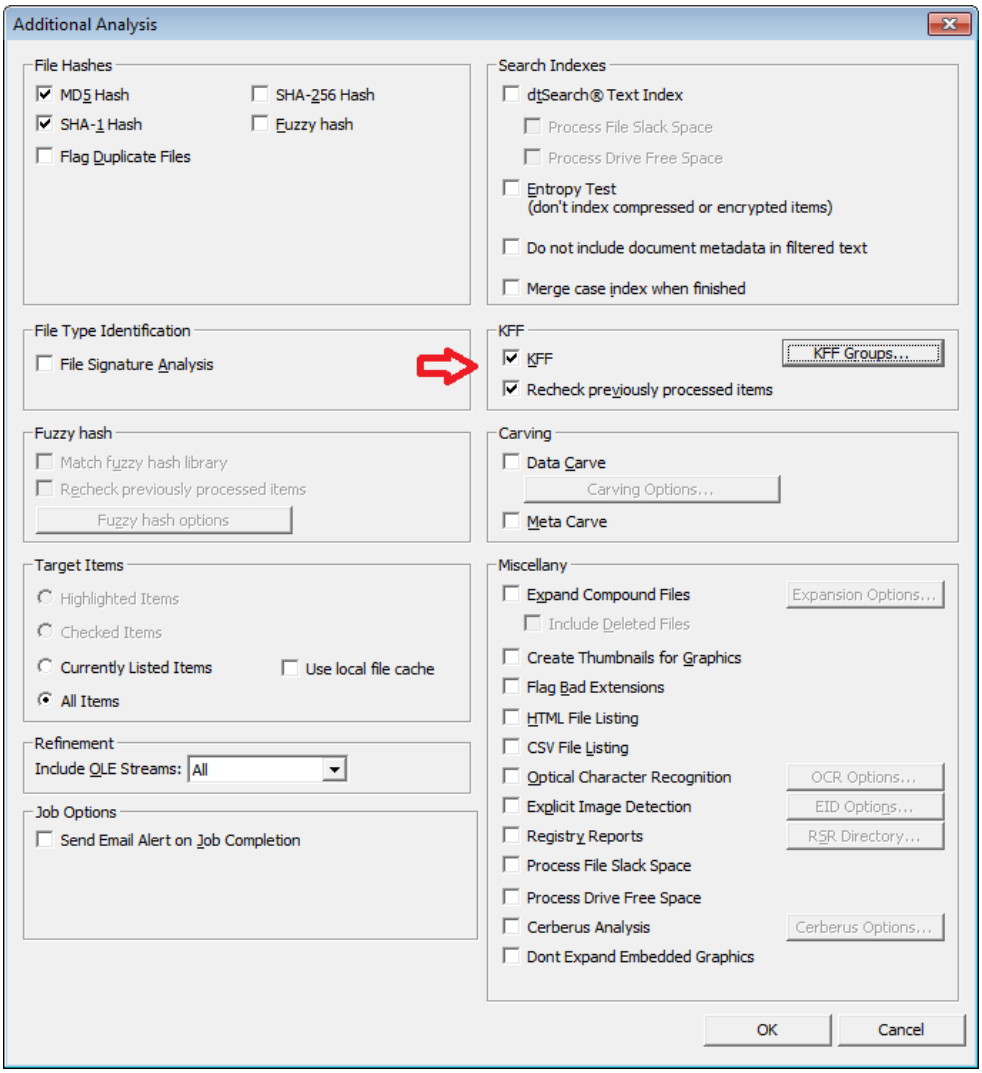


38. Click done.

39. Click on Evidence on the top of your FTK screen.

40.Click on Additional Analysis.

41. Checkmark the KFF and Recheck previously processed items.



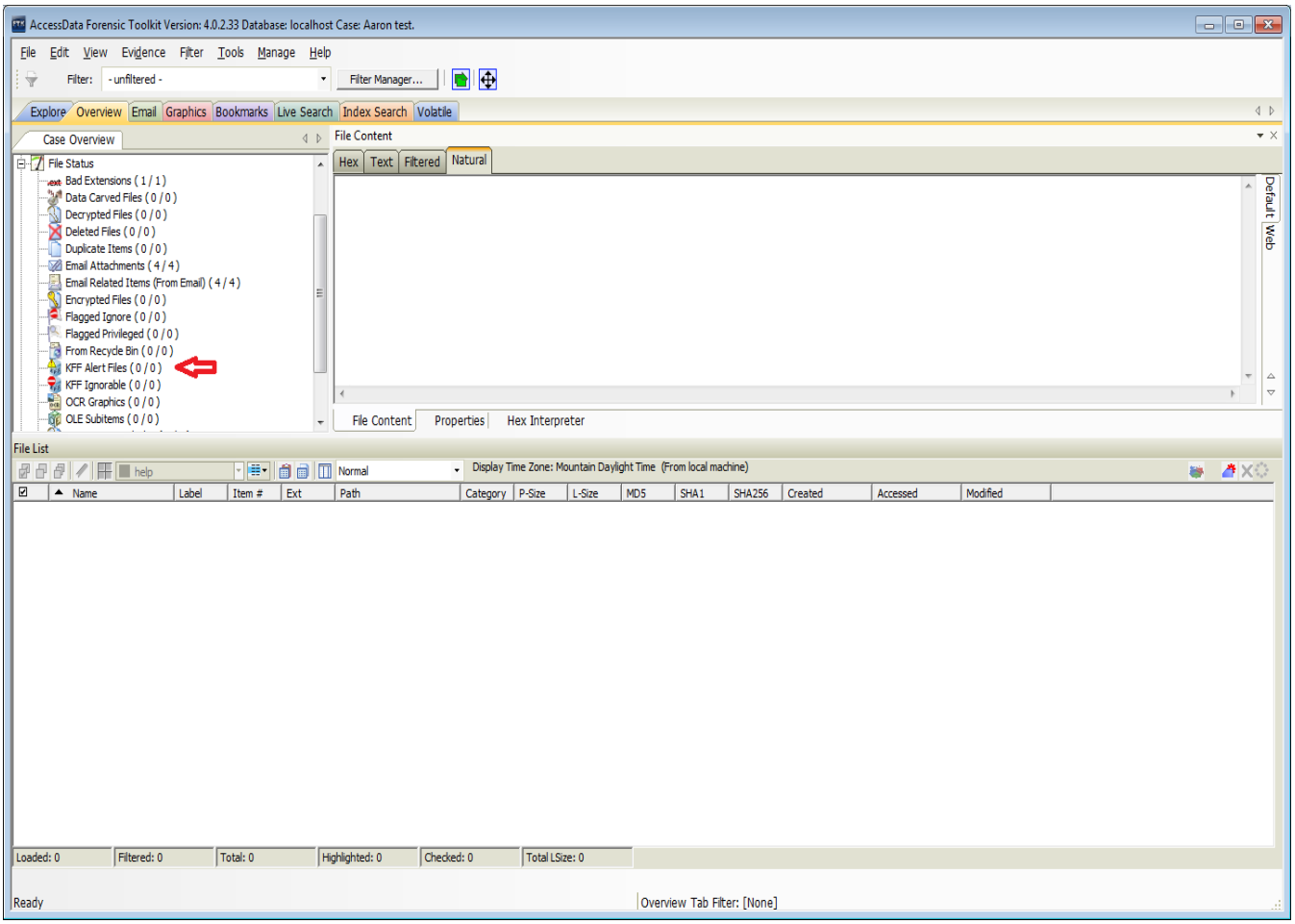
42. Click on the KFF Groups button to make sure your corre ct group is still checked.

43. Click done.

44. Click Ok at the bottom of the Additional Analysis to begin the analysis.

45. Once done go to your Overview tab in FTK.

46. Expand File Status and look at the KFF Alert Files.



47. Create a new column setting as you did in steps 2-8.

48. Expand the All Features list and select "Name"and "KFF Status" and "KFF Group".

49. This will show the correct column settings for running this in FTK.