Task 3  
Ms. Jones notifies you that the former employee has used an additional drive. She asks you to examine this new drive to determine whether it contains an account number the employee might have had access to. The account number, 461562, belongs to the senior vice president and is used to access the company’s banking service over the Internet.  
  
1. Start ProDiscover Basic. In the New Project tab, enter a project number, the project name C2Prj03, and a brief description, and then click Open. Save the project in your work folder by clicking File, Save Project from the menu.  
  
2. To add the evidence, click Action from the menu, point to Add, and click Image File. Navigate to your work folder, click the C2Prj03.dd file, and then click Open. Click Yes in the Auto Image Checksum message box, if necessary. Notice that the image file is a .dd file, not an .eve file. Like most forensics tools, ProDiscover can read standard UNIX .dd image files.  
  
3. To aid in your investigation, you might want to view graphics files on the drive. To do this, click to expand Content View in the tree view, click to expand Images, and then click the pathname containing the image file.  
  
4. Click View, Gallery View from the menu. Scroll through the graphics files on the drive image. You’ll need to search through all folders, which can take some time. If a file is of interest, click the check box next to it in the Select column. In the Add Comment dialog box that opens, enter a description and click OK. These notes are added to the ProDiscover report.  
  
5. This drive is related to the case in Task 2, so you’re still looking for occurrences of the word “book.” Open the Search dialog box, and repeat Steps 5 through 8 of Task 2 for this drive image. When you view the search results, click to select any files of interest (as described in Step 4), which opens the Add Comment dialog box where you can enter notes.  
  
6. Next, search for the account number Ms. Jones gave you. Click the Search toolbar button. Click the Content Search tab, if necessary, and type 461562 as the search keyword. Click to select the drive you’re searching, and then click OK. Click the Cluster Search tab, and repeat the search for the account number. Remember to select any files of interest and enter notes in the Add Comment dialog box.  
  
7. When you’re finished, click Report in the tree view. Scroll through the report to make sure all the items you found are listed.  
  
8. Next, click the Export toolbar button. In the Export dialog box, click the RTF Format option button, type Ch2Prj03Report in the File Name text box, and then click OK. (If you want to store the report in a different folder, click Browse and navigate to the new location.)  
  
9. Write a short memo to summarize what you found. Save the project and exit ProDiscover Basic.

You can continue for Task 3, 4, 5 and 6.

Task 4  
Sometimes discovery demands from law firms require you to recover only allocated data from a disk. This project shows you how to extract just the files that haven’t been deleted from an image.  
  
1. Start ProDiscover Basic. In the New Project tab, enter a project number, brief description, and the project name C2Prj04, and then click Open.  
  
2. In the tree view, click to expand Add, and then click Image File. Navigate to your work folder, click the C2Prj04.eve file, and then click Open. Click Yes in the Auto Image Checksum message box, if necessary. Save the project in your work folder.  
  
3. In the tree view, click to expand Content View, click to expand Images, and then click the pathname containing the image file. Notice the files visible in the work area.  
  
4. Click the column header Deleted to sort the files into YES and NO groups (see Figure 3.3). Figure 3.3 Deleted file displayed in the work area.  
  
5. To extract the allocated files from the image to your work folder, right-click each file containing NO in the Deleted column and click Copy File. (Note that in ProDiscover Basic, there’s no way to select multiple files at once. You must copy each allocated file separately.) When you’re finished, save the project and exit ProDiscover Basic.

Table

Description automatically generated

Figure 3.3 Deleted File Displayed in the Work Area

Task 5  
This project is a continuation from the previous project; you’ll create a report listing all the unallocated (deleted) files ProDiscover finds.  
  
1. Start ProDiscover Basic. Click the Open Project tab, and navigate to your work folder.  
  
2. Click the C2Prj04.dft file and click Open. Click Yes in the Auto Image Checksum message box, if necessary.  
  
3. If necessary, sort the files in the work area again by clicking the Deleted column header. Click the check box in the Select column next to all unallocated (deleted) files, as shown in Figure 3.4. As you click each check box, the Add Comment dialog box opens, where you can enter a description of each file. Figure 3.4 Selecting a file include in a report   
  
4. In the Investigator comments text box, add a comment noting that the file is deleted and indicating its file type, such as a Word document or an image file (.jpeg or .gif, for instance). Be sure to enter something meaningful by examining the file first.  
  
5. When you’re finished, click Report in the tree view. If you’re satisfied, export the report by clicking the Export toolbar button. In the Export dialog box, select the format option you want, type C2Prj05Report in the File Name text box, and then click OK. Save the project and exit ProDiscover Basic.

Graphical user interface, application

Description automatically generated

Figure 3.4 Selecting a file include in a report

Task 6  
In this project, another investigator asks you to examine an image and search for all occurrences of the following keywords:  
i) ANTONIO  
ii) HUGH EVANS  
iii) HORATIO  
  
1. Start ProDiscover Basic. In the New Project tab, enter a project number, brief description, and the project name, and then click Open.  
  
2. In the tree view, click to expand Add, and click Image File. Navigate to your work folder, click the C2Prj06.eve file, and click Open. Click Yes in the Auto Image Checksum message box, if necessary. Save the project in  
your work folder.  
  
3. Click the Search toolbar button. In the Search dialog box, type all keywords in the list box (placing each on a separate line), click to select the drive containing the image, and click OK.  
  
4. Examine the files in the search results pane. Select the ones that look interesting and enter notes in the Add Comment dialog box.  
  
5. Generate a report and export it, as explained in previous projects. Save the project and exit ProDiscover Basic.