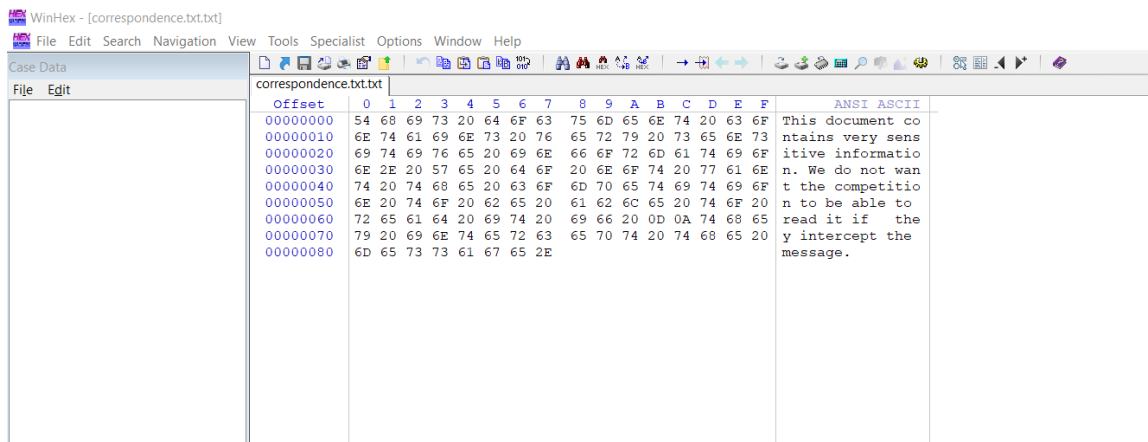


Complete hands-on project 9-1, 9-2, 9-3, 9-4

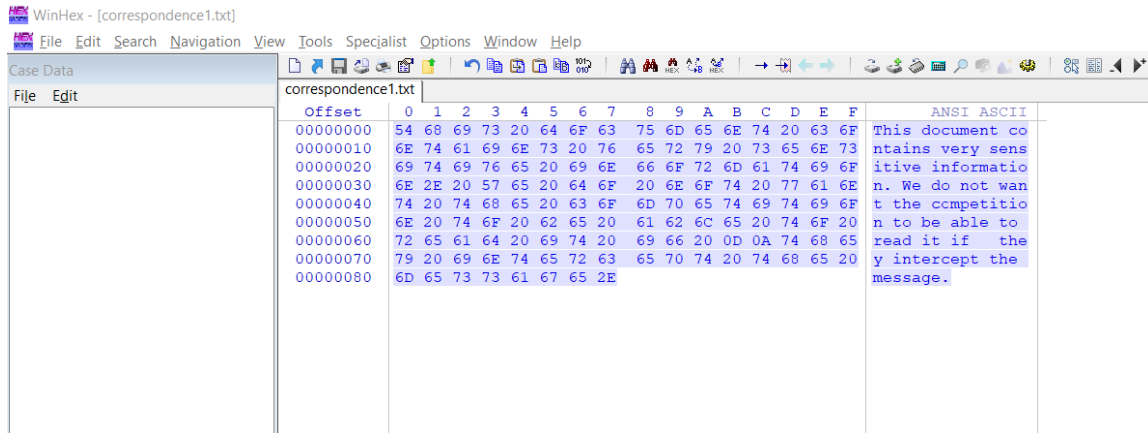
Hands-On Project 9-1

1. In a new text document, open Notepad and type the following: This paper includes highly confidential data. If the message is intercepted, we don't want the competition to be able to read it.
2. Save the file as correspondence.txt in your work folder, and then exit Notepad.
3. Start WinHex, using the Run as administrator option. (If necessary, when the UAC message box opens, click Yes.) Open the correspondence.txt file.



4. You used the left and right shift options in the in-chapter activity. The Circular left rotation option in the Modify Block Data dialog box is used for this project. Select All from the menu when you click Edit.
5. From the menu, select Edit, Modify Data. Click the Circular left rotation option button in the Modify Block Data dialog box, then click OK.
6. Save the file as correspondence1.txt, and exit WinHex.
7. Restart WinHex, and open correspondence1.txt. Click Edit, Select All from the menu.
8. Select Edit, Modify Data from the menu while the contents of the file are highlighted. If necessary, rotate the bits using the Circular left rotation option button in the Modify Block Data dialog box, then click OK. This process should be repeated seven times to ensure that the data can be recovered.

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)



9. When you have recovered the text to its readable state, save it as correspondence2.txt.

Version 11.9 of WinHex is a sophisticated file, disk, and RAM editor. It is a commercial gadget with a price range of \$60 to \$350. The cost is determined by the type of license purchased. The main functions of a personal license include cloning, erasing, viewing and altering files, including files that cannot be modified ordinarily, data recovery, and many more tasks. The professional license covers everything a personal license permits, as well as scripting and API functionality. The next feature of the specialist is the specialized menu, which allows the user to gather free, slack, and inter-partition space. There's also a new search option.

Finally, the forensic license type comes with the X-Ways Forensics feature, which provides a slew of new features. X-Ways Forensics is a specially designed environment for computer forensic experts. X-Ways also offers a trial edition for consumers to try out before purchasing the full version. The evaluation version of WinHex was utilized in this experiment to determine the most fundamental functionalities of WinHex and how well they perform.

Some of the feature of WinHex are:

- Editors for disks, files, and RAM
- WinHex is a binary editor that lets you access every aspect of a piece of media.
- Directory Browser for FAT and NTFS File Systems
- Lists all files and directories, including those that have been deleted, together with all of their metadata.
- Cleaning and erasing of hard drives
- Wipes the drive and allows the user to choose what to overwrite it with: random ones zeros or any sequence. The user can also select the number of wipes to be used by the utility.
- Data Interpreter and Data Analysis are two terms that are often used interchangeably.
- Can understand any type of data and determine what type of binary data the user possesses.

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

WinHex can be used by a forensic investigator to see a directory in the FAT or NTFS file systems. System of files This includes files that have been removed from the system. The investigator will be able to see if any files have been erased as a result of this. Then they could utilize data recovery to recover the information that has been lost. The sectors connected with that file have been removed, and the sectors associated with that file have been marked as unallocated. The file and its contents can then be seen using WinHex to figure out why the file was removed.

WinHex can also be used to get a machine ready for forensics. Win Hex's

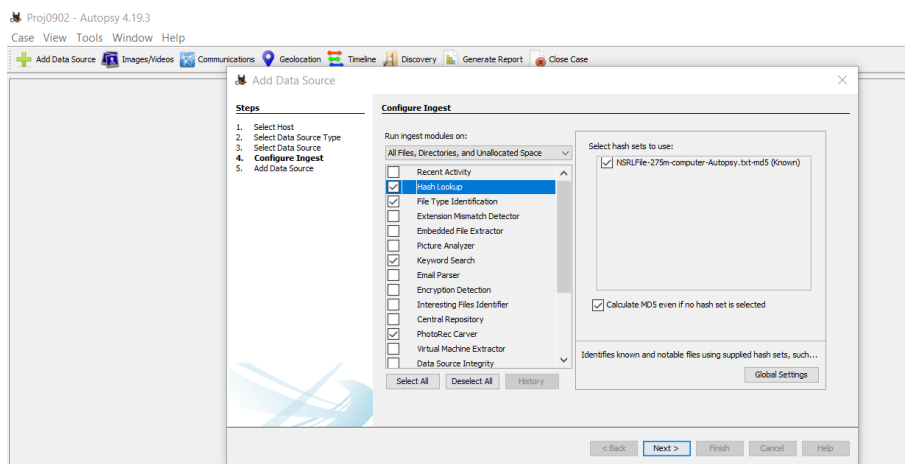
wiping option lets the user to wipe a file or drive as many times as they want. In WinHex, the wipe option can be changed to any value. A random wipe is included in a sequence of ones and zeros. This is crucial because the number of times a file or drive is wiped is proportional to the size of the file or drive the importance of the info in a file or on a piece of media.

Hands-On Projects 9-2

1. To begin, open Autopsy for Windows. To start a new case, click the Create New Case button. Enter Proj0902 in the Case Name text box in the New Case Information window, and then click Browse next to the Base Directory text box. Go to your work folder and click it, then click Next. Type Proj0902 in the Case Number text box and your name in the Examiner text box in the Additional Information window, then click Finish.

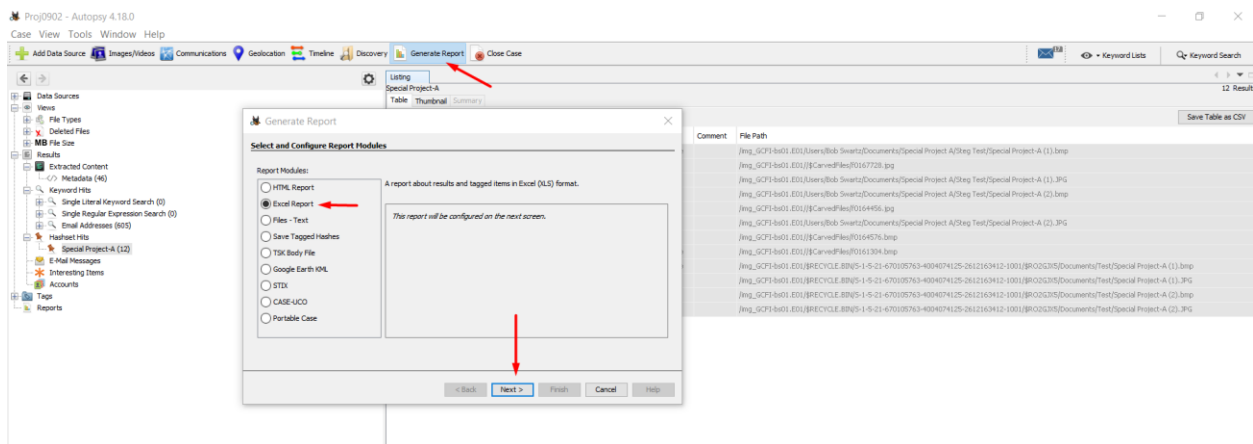
2. In the Select Data Source window, click the Browse button next to the "Browse for an image file" text box, navigate to your work folder and click the GCFI-bs01.E01 file, and then click Open. Click Next.

3. Select the Hash Lookup check box in the Configure Ingest Modules window. Clear the NISTFile-nnm.txt-md5 check box in the "Select known hash databases to utilize" list box, then check the Special Project-A box. Select the File Type Identification, Keyword Search, PhotoRec Carver, and E01 Verifier check boxes under the Hash Lookup check box. Click Next, then Finish after checking the Calculate MD5 even if no hash database is selected check box.



Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

- When Autopsy finishes its analysis, go to the Tree Viewer pane, and expand Results, Hashset Hits to see the matching files found in the GCFI-bs01.E01 image.
- In the Result Viewer pane, Ctrl+click all files. Right-click this selection, point to Tag Results and Quick Tag, and click Special Project-A.
- At the top, select Generate Report. Click the Results - Excel option button in the Report Modules section of the Generate Report box, then Next. Click the Tagged Results option button in the Configure Artifact Reports window, check the Special Project-A check box, and then click Finish.



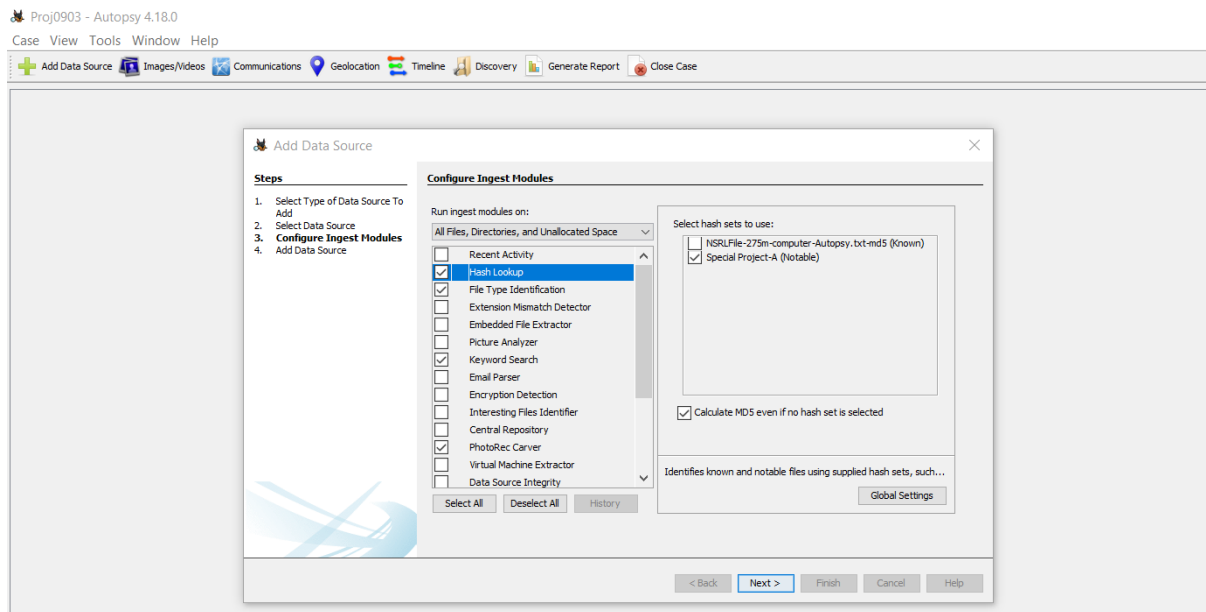
- In the Report Generation Progress window, click the Results - Excel pathname once the report has been generated. Examine the contents of the Tagged Files sheet in the Excel file. Review the hash values in column I, which is called Hash. Save the Excel file as Proj0902-Report in your work folder when you're finished.
- Click Close Case, and leave Autopsy running for the next project.

Hands-On Project 9-3

- Start the Windows version of Autopsy. To start a new case, click the Create New Case button. Enter Proj0903 in the Case Name text box in the New Case Information window, and then click Browse next to the Base Directory text box. Go to your work folder and click it, then click Next. Type Proj0903 in the Case Number text box and your name in the Examiner text box in the Additional Information window, then click Finish.

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

2. In the Select Data Source window, click the Browse button next to the “Browse for an image file” text box, navigate to your work folder and click the GCFI-bs01.E01 file, and then click Open. Click Next.
3. Select the Hash Lookup check box in the Configure Ingest Modules window. Clear the NISTFile-nnm.txt-md5 check box in the "Select known hash databases to utilize" list box, then check the Special Project-A box. Select the File Type Identification, Keyword Search, PhotoRec Carver, and E01 Verifier check boxes under the Hash Lookup check box. Click Next, then Finish after checking the Calculate MD5 even if no hash database is selected check box.

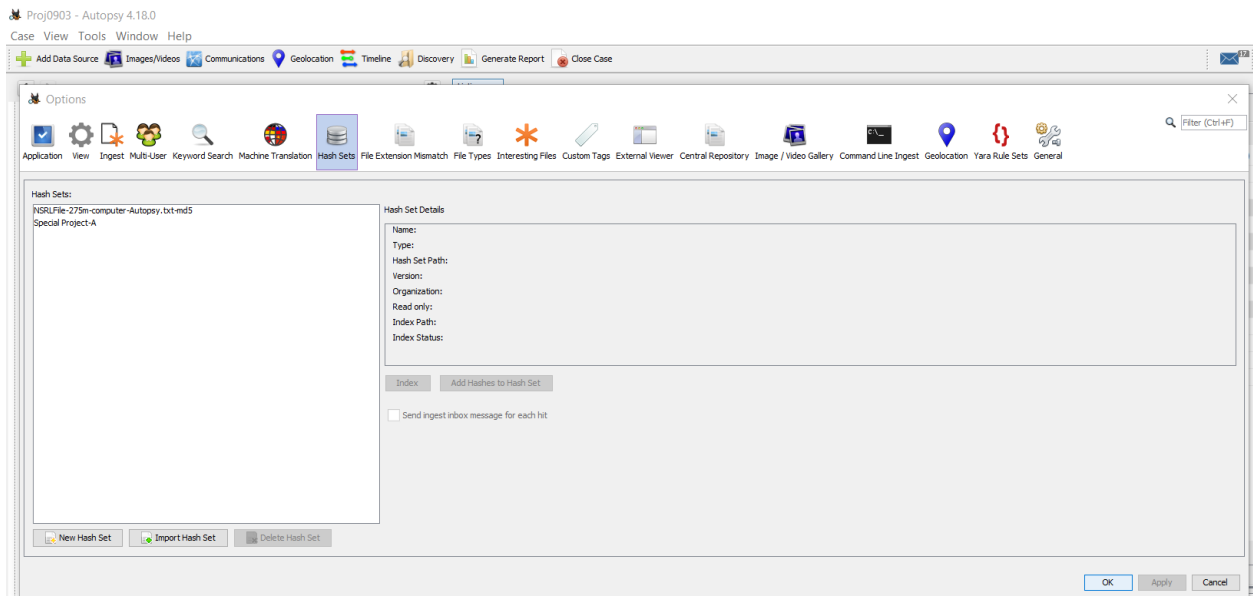


4. When Autopsy finishes its analysis, go to the Tree Viewer pane, expand Data Sources, and navigate to the path GCFI-bs01.E01\Users\Bob Swartz\Documents\Special Project A\Design Specs.
5. In the Result Viewer pane, Ctrl+click all Special Project A files with a .docx extension. Right-click this selection, point to Tag File and Quick Tag, and click Special Project-A.
6. Click Generate Report at the top. In the Generate Report window, click the Results - Excel option button in the Report Modules section, and then click Next. In the Configure Artifact Reports window, click the Tagged Results option button, click the Special Project-A check box, and then click Finish.
7. When the report is finished, close the Report Generation Progress box by clicking the Results - Excel pathname. Examine the contents of the Tagged Files sheet in the Excel file. Review the hash values in column I, which is called Hash. Save the Excel file as Proj0903-

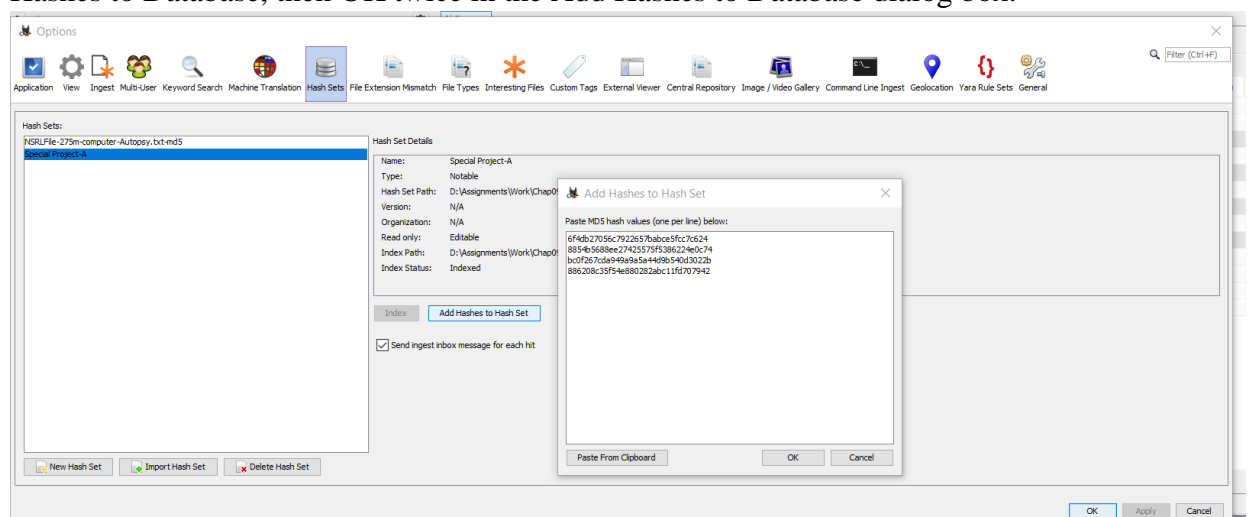
Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

Report in your work folder when you're finished. Keep this file open for the rest of the process.

8. In column I in the Tagged Files sheet, copy the four MD5 hash values in rows 2 through 5.
9. Click Tools, Options from the Autopsy menu, and in the Options window, click the Hash Databases icon.



- 10 Click Special Project-A in the Hash Databases list box, and then click Add Hashes to Database in the Hash Database Information section. Click Paste from Clipboard, then Add Hashes to Database, then OK twice in the Add Hashes to Database dialog box.

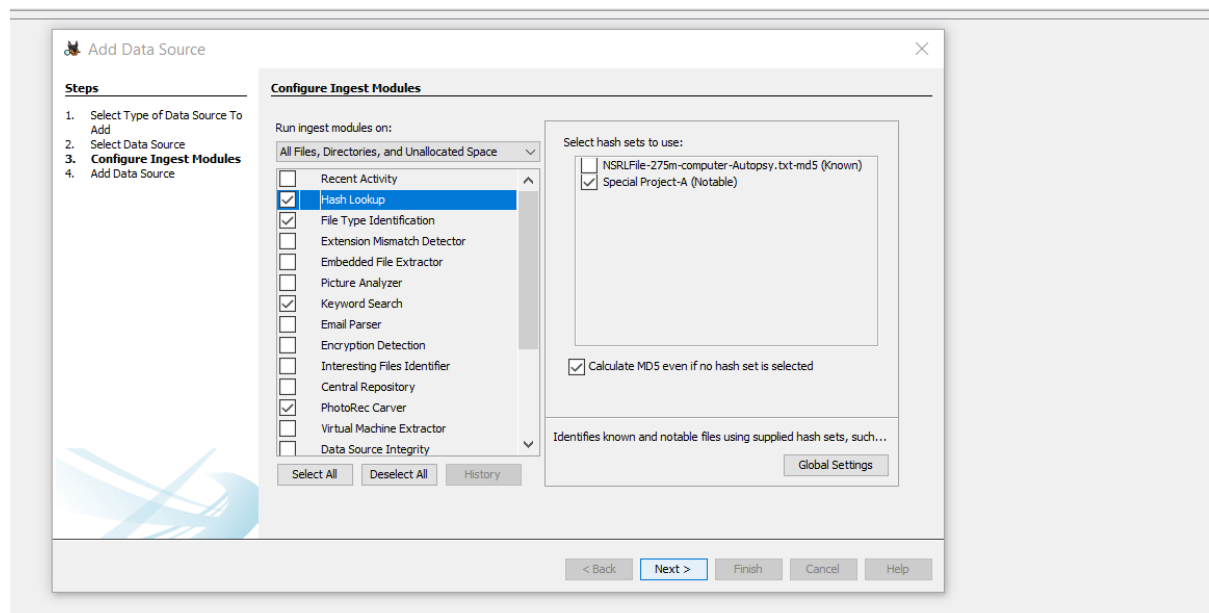


- 11 . Exit Excel, click Close Case in Autopsy, and then leave Autopsy running for the next project.

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

Hands-On Project 9-4

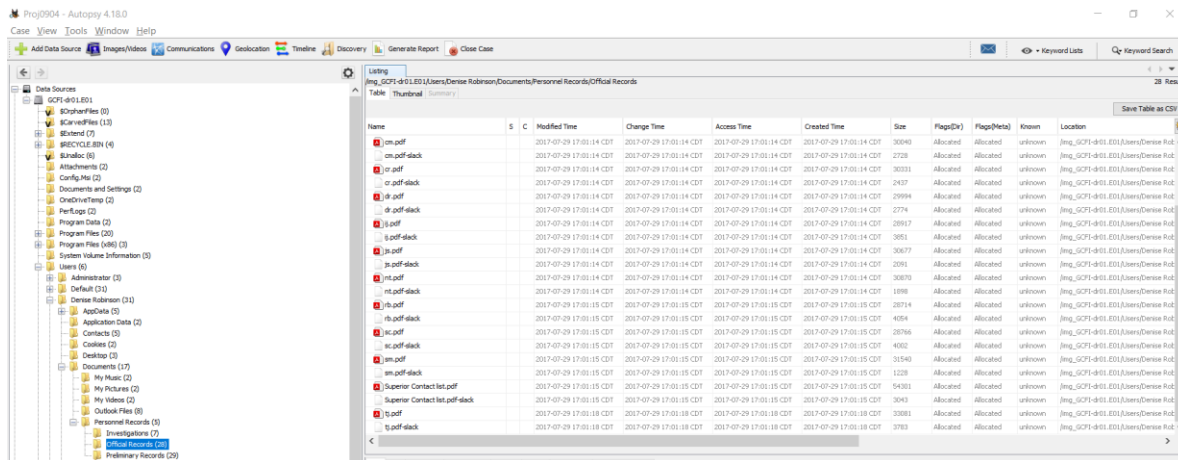
1. If necessary, start Autopsy for Windows. To start a new case, click the Create New Case button. Enter Proj0904 in the Case Name text box in the New Case Information window, and then click Browse next to the Base Directory text box. Go to your work folder and click it, then click Next. Type Proj0904 in the Case Number text box and your name in the Examiner text box in the Additional Information window, then click Finish.
2. In the Select Data Source window, click the Browse button next to the "Browse for an image file" text box, navigate to and click your work folder and the GCFI-dr01.E01 file, and then click Open. Click Next.
3. Select the Hash Lookup check box in the Configure Ingest Modules window. Click the NISTFile-nnm.txt-md5 check box in the "Select known hash databases to utilize" section, then clear the Special Project-A check box. Select the check boxes for File Type Identification, Keyword Search, and E01 Verifier on the left. Click the Calculate MD5 even if no hash database is specified check box under "Select known BAD hash databases to utilize," then Next and Finish.



4. When Autopsy finishes its analysis, go to the Tree Viewer pane, and click to expand Data Sources. Navigate to the path GCFI-dr01.E01\Users\Denise Robinson\Documents\Special Project A\Personnel Records.

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

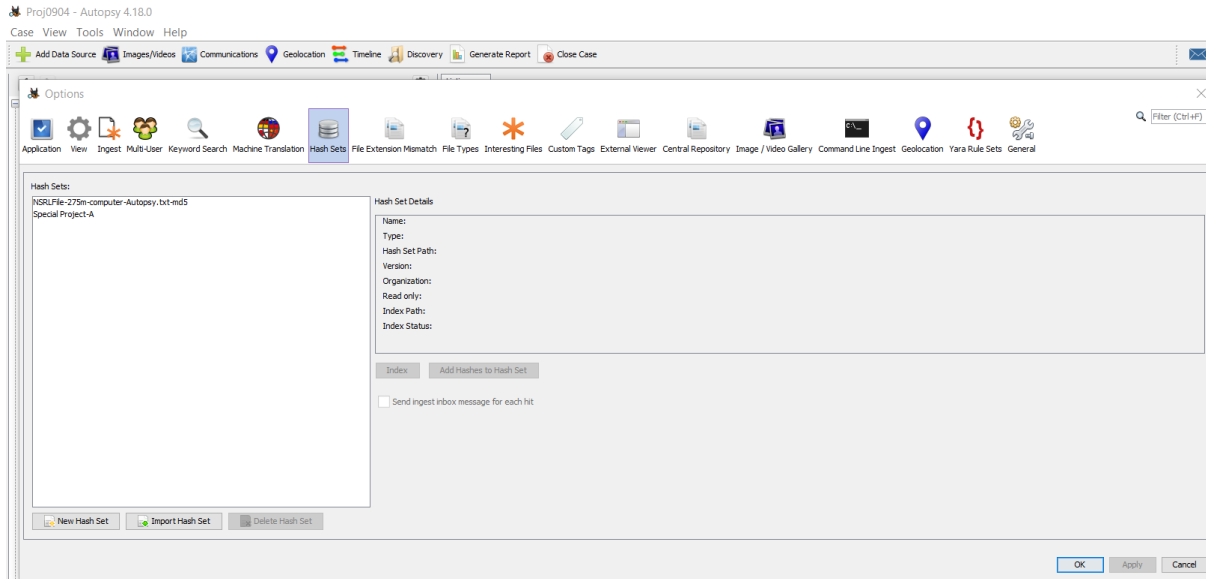
5. In the Personnel Records folder, examine the contents of the Investigations subfolder. In the Result Viewer pane, Ctrl+click any files with the extensions .ods, .odt, and .pdf. Ignore all files beginning with the tilde (~) character and those with the extensions .ods-slack, .odt-slack, and .pdf-slack.
6. Right-click the highlighted files, select Tag File from the context menu, and then select Tag and Comment. Click the New Tag Name button, write Superior-Personnel-Records in the Tag Name text box, and then click OK twice in the Create Tag dialog box.
7. Examine the contents of the Official Records subfolder in the Personnel Records folder. Click to choose any files with the extensions.ods,.odt, or.pdf in the Result Viewer box. (All files beginning with the tilde () character, as well as the extensions.ods-slack,.odt-slack, and.pdf-slack, should be ignored.)



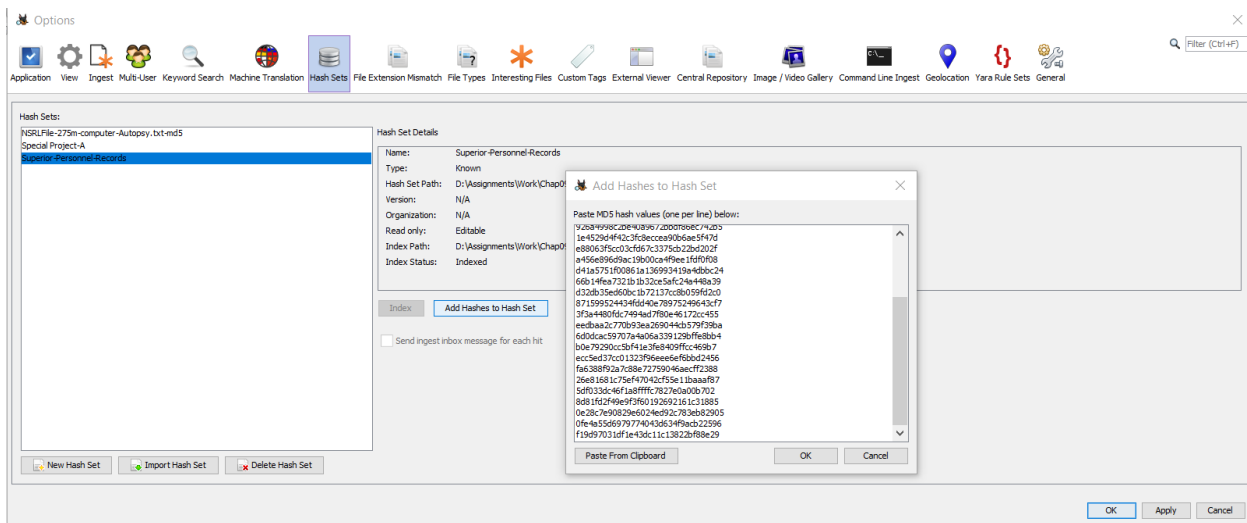
Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dx)	Flags(Mx)	Known	Location
am.pdf			2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	30962	Allocated	Allocated	unknown	Img_SC271-d-011.ED1\Users\Robinson\Documents\Personnel Records\Official Records
am.pdf-slack			2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	2728	Allocated	Allocated	unknown	Img_SC271-d-011.ED1\Users\Robinson\Documents\Personnel Records\Official Records
ar.pdf			2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	30333	Allocated	Allocated	unknown	Img_SC271-d-011.ED1\Users\Robinson\Documents\Personnel Records\Official Records
ar.pdf-slack			2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	2437	Allocated	Allocated	unknown	Img_SC271-d-011.ED1\Users\Robinson\Documents\Personnel Records\Official Records
is.pdf			2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	29994	Allocated	Allocated	unknown	Img_SC271-d-011.ED1\Users\Robinson\Documents\Personnel Records\Official Records
is.pdf-slack			2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	2774	Allocated	Allocated	unknown	Img_SC271-d-011.ED1\Users\Robinson\Documents\Personnel Records\Official Records
nt.pdf			2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	28917	Allocated	Allocated	unknown	Img_SC271-d-011.ED1\Users\Robinson\Documents\Personnel Records\Official Records
nt.pdf-slack			2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	3651	Allocated	Allocated	unknown	Img_SC271-d-011.ED1\Users\Robinson\Documents\Personnel Records\Official Records
ru.pdf			2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	30037	Allocated	Allocated	unknown	Img_SC271-d-011.ED1\Users\Robinson\Documents\Personnel Records\Official Records
ru.pdf-slack			2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	2091	Allocated	Allocated	unknown	Img_SC271-d-011.ED1\Users\Robinson\Documents\Personnel Records\Official Records
sc.pdf			2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	30070	Allocated	Allocated	unknown	Img_SC271-d-011.ED1\Users\Robinson\Documents\Personnel Records\Official Records
sc.pdf-slack			2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	2017-07-29 17:01:14 CDT	1898	Allocated	Allocated	unknown	Img_SC271-d-011.ED1\Users\Robinson\Documents\Personnel Records\Official Records
sm.pdf			2017-07-29 17:01:15 CDT	2017-07-29 17:01:15 CDT	2017-07-29 17:01:15 CDT	2017-07-29 17:01:15 CDT	28714	Allocated	Allocated	unknown	Img_SC271-d-011.ED1\Users\Robinson\Documents\Personnel Records\Official Records
sm.pdf-slack			2017-07-29 17:01:15 CDT	2017-07-29 17:01:15 CDT	2017-07-29 17:01:15 CDT	2017-07-29 17:01:15 CDT	4094	Allocated	Allocated	unknown	Img_SC271-d-011.ED1\Users\Robinson\Documents\Personnel Records\Official Records
ts.pdf			2017-07-29 17:01:15 CDT	2017-07-29 17:01:15 CDT	2017-07-29 17:01:15 CDT	2017-07-29 17:01:15 CDT	28786	Allocated	Allocated	unknown	Img_SC271-d-011.ED1\Users\Robinson\Documents\Personnel Records\Official Records
ts.pdf-slack			2017-07-29 17:01:15 CDT	2017-07-29 17:01:15 CDT	2017-07-29 17:01:15 CDT	2017-07-29 17:01:15 CDT	4052	Allocated	Allocated	unknown	Img_SC271-d-011.ED1\Users\Robinson\Documents\Personnel Records\Official Records
Superior Contact list.pdf			2017-07-29 17:01:15 CDT	2017-07-29 17:01:15 CDT	2017-07-29 17:01:15 CDT	2017-07-29 17:01:15 CDT	31540	Allocated	Allocated	unknown	Img_SC271-d-011.ED1\Users\Robinson\Documents\Personnel Records\Official Records
Superior Contact list.pdf-slack			2017-07-29 17:01:15 CDT	2017-07-29 17:01:15 CDT	2017-07-29 17:01:15 CDT	2017-07-29 17:01:15 CDT	1228	Allocated	Allocated	unknown	Img_SC271-d-011.ED1\Users\Robinson\Documents\Personnel Records\Official Records
ts.pdf			2017-07-29 17:01:18 CDT	2017-07-29 17:01:18 CDT	2017-07-29 17:01:18 CDT	2017-07-29 17:01:18 CDT	54361	Allocated	Allocated	unknown	Img_SC271-d-011.ED1\Users\Robinson\Documents\Personnel Records\Official Records
ts.pdf-slack			2017-07-29 17:01:18 CDT	2017-07-29 17:01:18 CDT	2017-07-29 17:01:18 CDT	2017-07-29 17:01:18 CDT	3043	Allocated	Allocated	unknown	Img_SC271-d-011.ED1\Users\Robinson\Documents\Personnel Records\Official Records
ts.pdf			2017-07-29 17:01:18 CDT	2017-07-29 17:01:18 CDT	2017-07-29 17:01:18 CDT	2017-07-29 17:01:18 CDT	33881	Allocated	Allocated	unknown	Img_SC271-d-011.ED1\Users\Robinson\Documents\Personnel Records\Official Records
ts.pdf-slack			2017-07-29 17:01:18 CDT	2017-07-29 17:01:18 CDT	2017-07-29 17:01:18 CDT	2017-07-29 17:01:18 CDT	3783	Allocated	Allocated	unknown	Img_SC271-d-011.ED1\Users\Robinson\Documents\Personnel Records\Official Records

8. Right-click the highlighted files, point to Tag File and then Quick Tag, and click Superior-Personnel-Records. Click OK twice.
9. Repeat Steps 7 and 8 for the Preliminary Records subfolder.
10. At the top, select Generate Report. Click the Results - Excel option button in the Report Modules section of the Generate Report box, then Next. Click the Tagged Results option button in the Configure Artifact Reports window, check the Superior-Personnel-Records check box, and then click Finish.
11. In the Report Generation Progress Complete window, click the Results - Excel link to open the Excel report. Examine the contents of the Tagged Files sheet, scroll to column I labeled Hash, and then save the file as Proj0904-Report in your work folder. Leave this file open for the next steps.
12. Navigate to column I again, and copy the four MD5 hash values in rows 2 through 29.
13. Click Tools, Options from the Autopsy menu, and in the Options window, click the Hash Databases icon.

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)



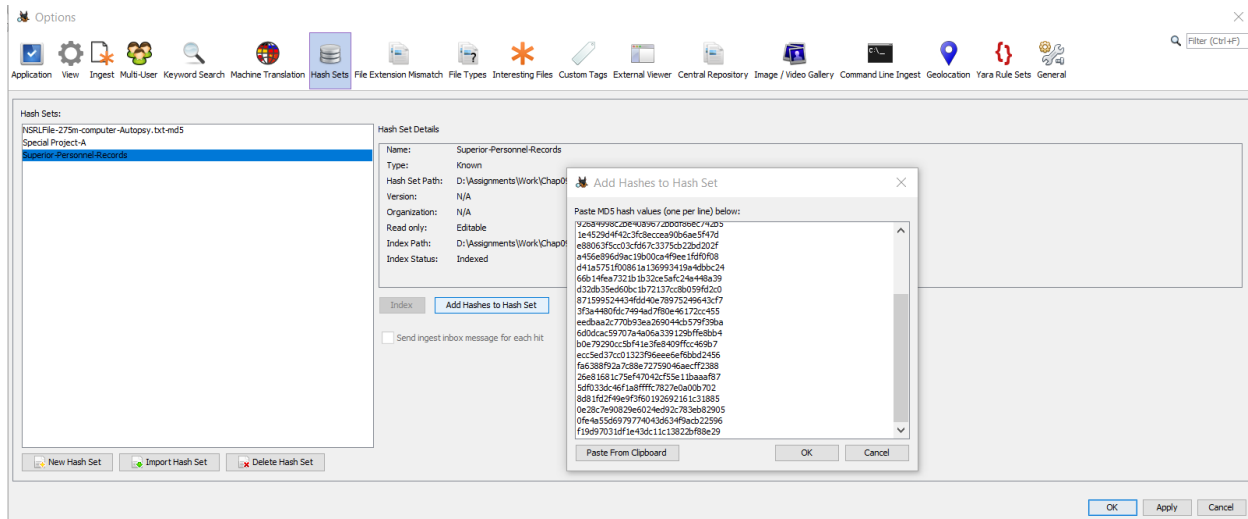
14. Click the new database button in the Hash Databases list box. In the Create Hash Database dialog box, in the Hash Set Name text box, type Superior-Personnel-Records and click Save as. Click Save in the Save dialog box, and then click Known Bad in the Create Hash Database dialog box, then OK.
15. In the Hash Database Information section, click Add Hashes to Database. In the Add Hashes to Database dialog box, click Paste from Clipboard, click Add Hashes to Database, and click OK twice.



16. When the report is finished, close the Report Generation Progress box by clicking the Results - Excel pathname. Examine the contents of the Tagged Files sheet in the Excel file. Review the hash values in column I, which is called Hash. When you're finished,

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

- save the Excel file in your work folder as Proj0904-Report. Keep this file open for the rest of the process.
17. In column I in the Tagged Files sheet, copy the MD5 hash values in rows 2 through 29
 18. Click Tools, Options from the Autopsy menu, and in the Options window, click the Hash Databases icon.
 19. In the Hash Databases list box, click Superior-Personnel-Records, and in the Hash Database Information section, click Add Hashes to Database. In the Add Hashes to Database dialog box, click Paste from Clipboard, click Add Hashes to Database, and click OK twice.



20. Exit Excel, and in Autopsy, click Close Case. Click Close again in the Welcome window, and then click Case and Exit.

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)