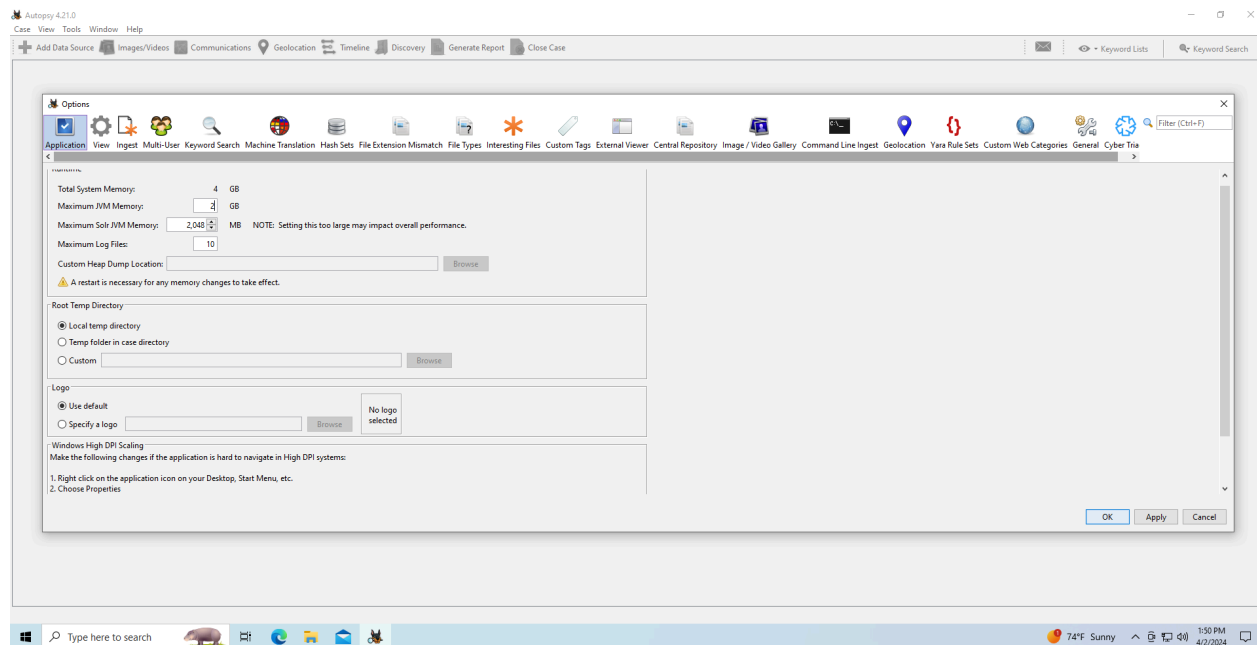
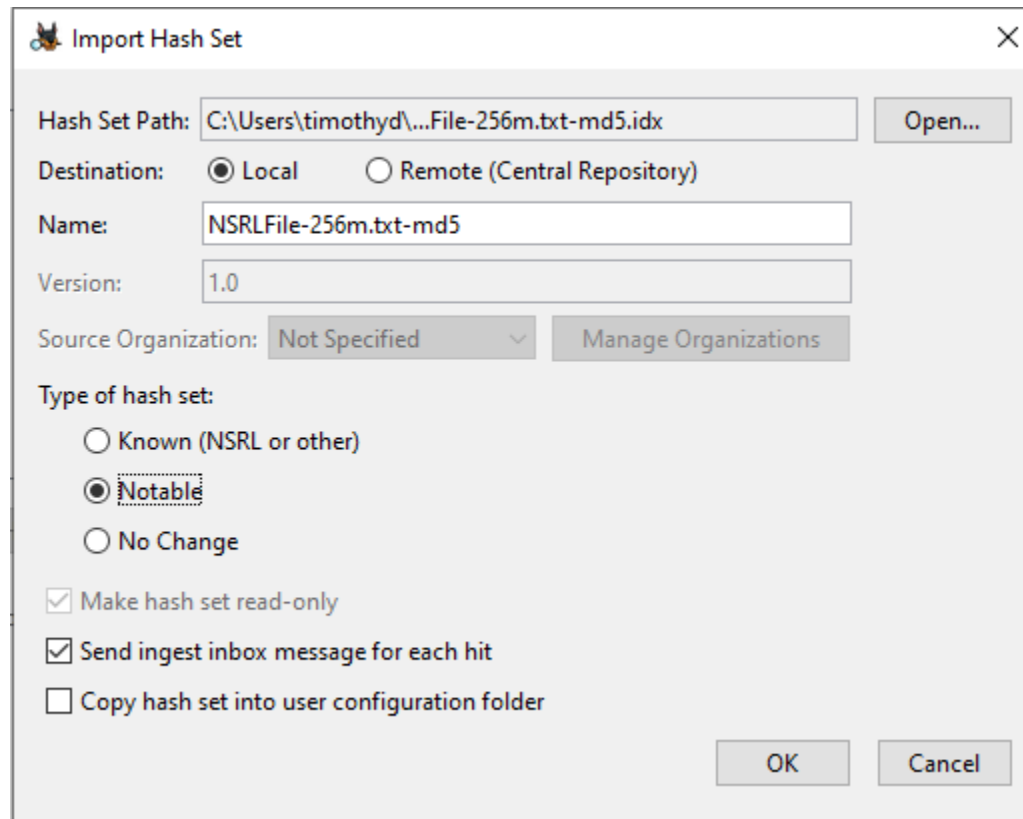


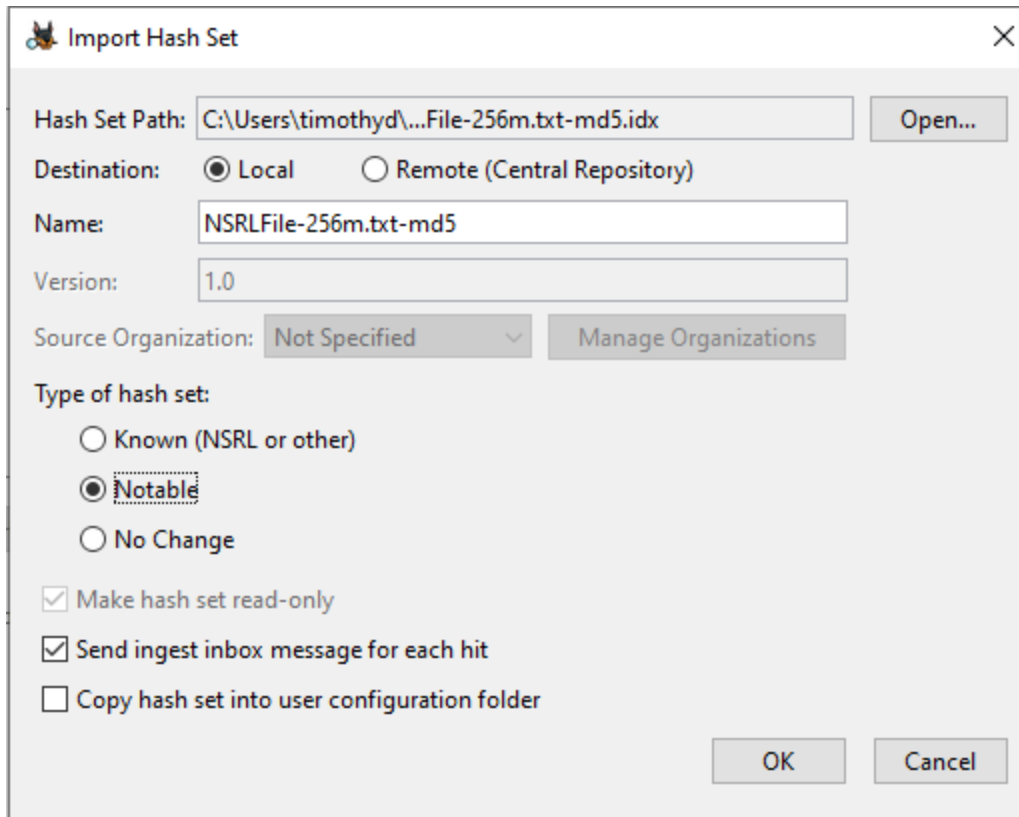
Task 1:



In this step, I have downloaded the NSRL. I am now in Autopsy and increasing the Max JVM Memory to 2 GB.



Here I am importing the database into Autopsy.



Import Hash Set

Hash Set Path:

Destination: ☒ Local ☐ Remote (Central Repository)

Name:

Version:

Source Organization:

Type of hash set:

☐ Known (NSRL or other)

☒ **Notable**

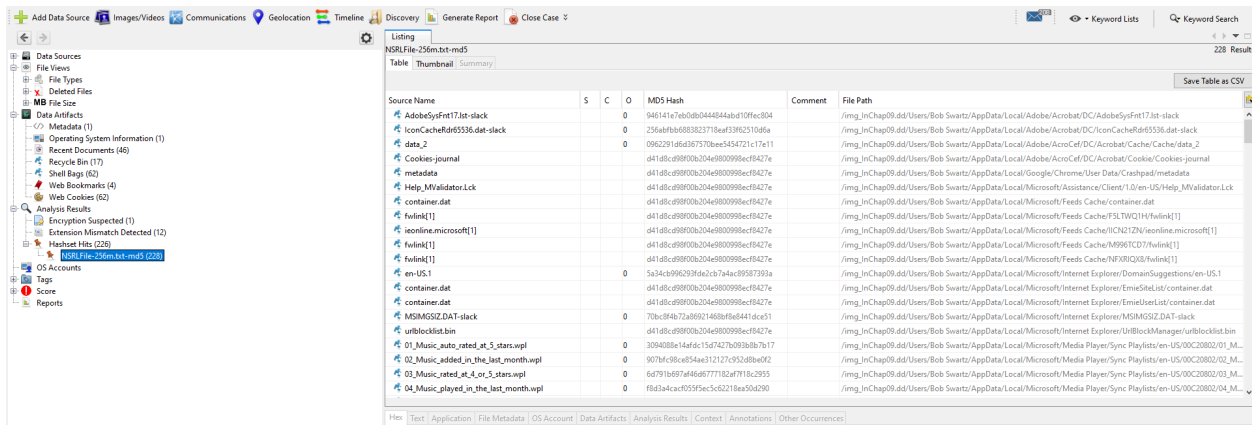
☐ No Change

☒ Make hash set read-only

☒ Send ingest inbox message for each hit

☐ Copy hash set into user configuration folder

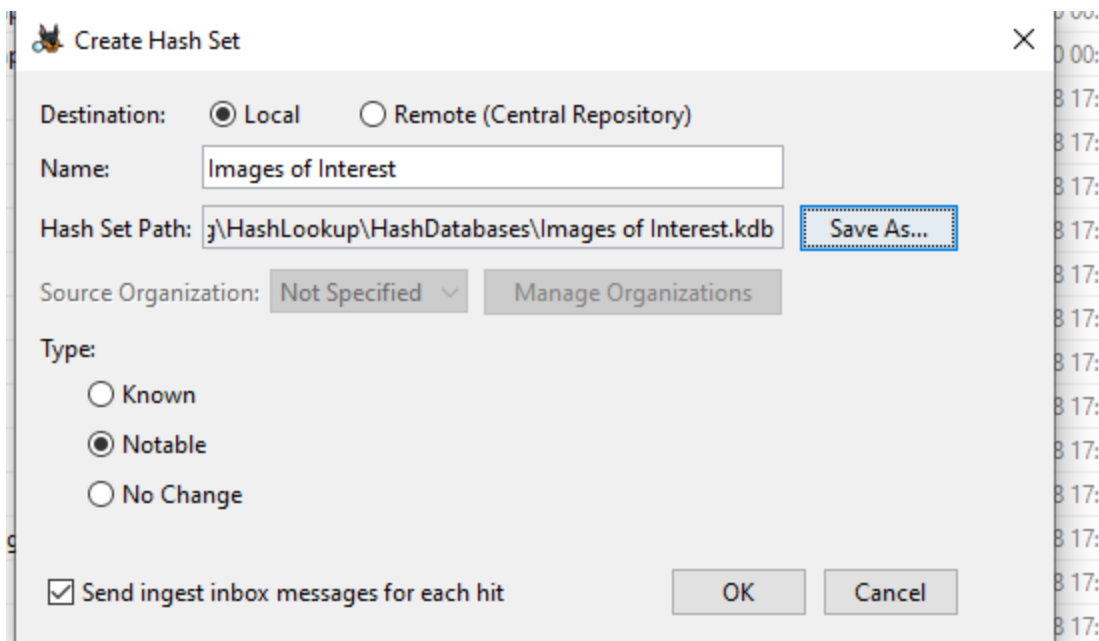
Here I have created a new case and added the InChapter09.dd file.



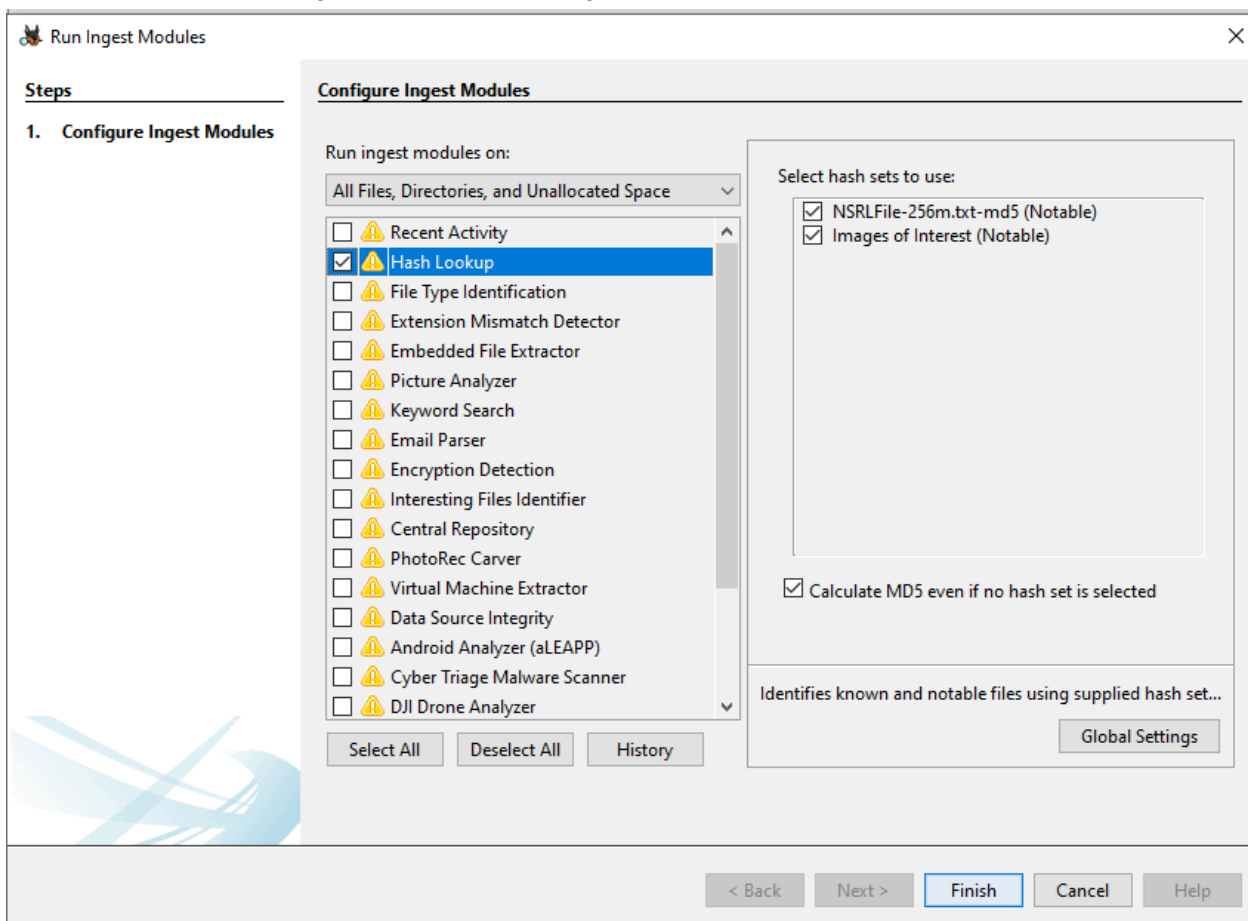
Listing
NSRFile-256m.txt-md5
228 Results

Source Name	S	C	O	MD5 Hash	Comment	File Path
AdobeSysFrt17.lst-slack	0			9461417eb0db0444844bd10fec804		/img_inChap09.dd/Users/Bob Swartz/AppData/Local/Adobe/SysFrt17.lst-slack
iconCacheHd5536.dat-slack	0			256abfb683823778eaf33962510a6a		/img_inChap09.dd/Users/Bob Swartz/AppData/Local/Adobe/Acrobat/DC/iconCacheHd5536.dat-slack
data_2	0			096229186d367570bee5454721c17e11		/img_inChap09.dd/Users/Bob Swartz/AppData/Local/Adobe/Acrobat/DC/Acrobat/Cache/Cache/data_2
Cookies-journal				4d18fc49890b204a9800999ecf9427e		/img_inChap09.dd/Users/Bob Swartz/AppData/Local/Adobe/Acrobat/DC/Acrobat/Cookies-journal
metadata				4d18fc49890b204a9800999ecf9427e		/img_inChap09.dd/Users/Bob Swartz/AppData/Local/Google/Chrome/User Data/Cached/metadata
Help_MValidator.Lck				4d18fc49890b204a9800999ecf9427e		/img_inChap09.dd/Users/Bob Swartz/AppData/Local/Microsoft/Assistance/Client/1.0/en-US/Help_MValidator.Lck
container.dat				4d18fc49890b204a9800999ecf9427e		/img_inChap09.dd/Users/Bob Swartz/AppData/Local/Microsoft/Feeds/Cache/container.dat
fwlink[1]				4d18fc49890b204a9800999ecf9427e		/img_inChap09.dd/Users/Bob Swartz/AppData/Local/Microsoft/Feeds/Cache/FSLTWQ1H/fwlink[1]
ieonline.microsoft[1]				4d18fc49890b204a9800999ecf9427e		/img_inChap09.dd/Users/Bob Swartz/AppData/Local/Microsoft/Feeds/Cache/ICN127N/ieonline.microsoft[1]
fwlink[1]				4d18fc49890b204a9800999ecf9427e		/img_inChap09.dd/Users/Bob Swartz/AppData/Local/Microsoft/Feeds/Cache/M996TC07/fwlink[1]
fwlink[1]				4d18fc49890b204a9800999ecf9427e		/img_inChap09.dd/Users/Bob Swartz/AppData/Local/Microsoft/Feeds/Cache/NF9RQ103/fwlink[1]
en-US.1	0			5a34c996293f6d2cb7a4ac89587393a		/img_inChap09.dd/Users/Bob Swartz/AppData/Local/Microsoft/Internet Explorer/DomainSuggestions/en-US.1
container.dat				4d18fc49890b204a9800999ecf9427e		/img_inChap09.dd/Users/Bob Swartz/AppData/Local/Microsoft/Internet Explorer/EmieSiteList/container.dat
container.dat				4d18fc49890b204a9800999ecf9427e		/img_inChap09.dd/Users/Bob Swartz/AppData/Local/Microsoft/Internet Explorer/EmieSiteList/container.dat
MSGSSZ.DAT-slack	0			70bc984b72a89921488b9fd441a0e51		/img_inChap09.dd/Users/Bob Swartz/AppData/Local/Microsoft/Internet Explorer/MSGSSZ.DAT-slack
urlblocklist.bin				4d18fc49890b204a9800999ecf9427e		/img_inChap09.dd/Users/Bob Swartz/AppData/Local/Microsoft/Internet Explorer/UrlBlockManager/urlblocklist.bin
01_Music_auto_rated_at_5_stars.wpl	0			30a4080e14fd4c15d74276093b67b17		/img_inChap09.dd/Users/Bob Swartz/AppData/Local/Microsoft/Media Player/Sync Playlists/en-US/00C20802/01_M...
02_Music_added_in_the_last_month.wpl	0			907bf98ce854a43121271c95248be0f2		/img_inChap09.dd/Users/Bob Swartz/AppData/Local/Microsoft/Media Player/Sync Playlists/en-US/00C20802/02_M...
03_Music_rated_at_4_or_5_stars.wpl	0			6d791b697a46d6777132af7f18c2955		/img_inChap09.dd/Users/Bob Swartz/AppData/Local/Microsoft/Media Player/Sync Playlists/en-US/00C20802/03_M...
04_Music_played_in_the_last_month.wpl	0			f8d34cac49595ec5c0218a504590		/img_inChap09.dd/Users/Bob Swartz/AppData/Local/Microsoft/Media Player/Sync Playlists/en-US/00C20802/04_M...

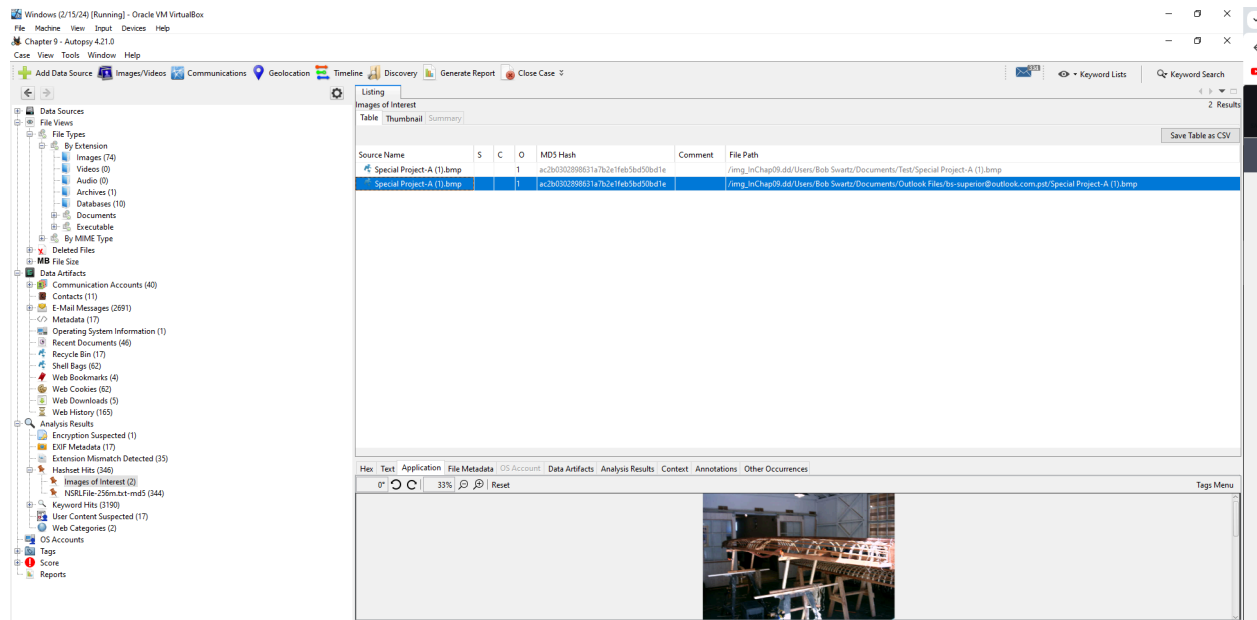
In this step, we can see that Autopsy identified the hash hits.



In this step, I am creating a hash set and filing it to the hash database.

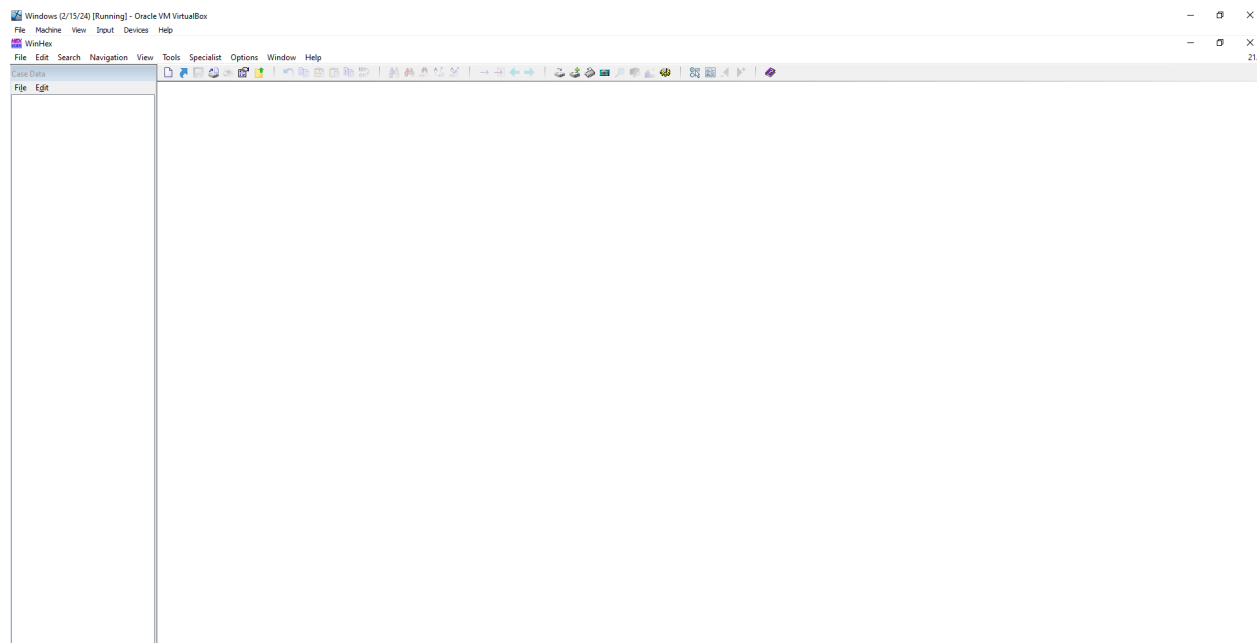


In this step, I am in “Run Ingest Modules” and can see that Images of Interest are listed.

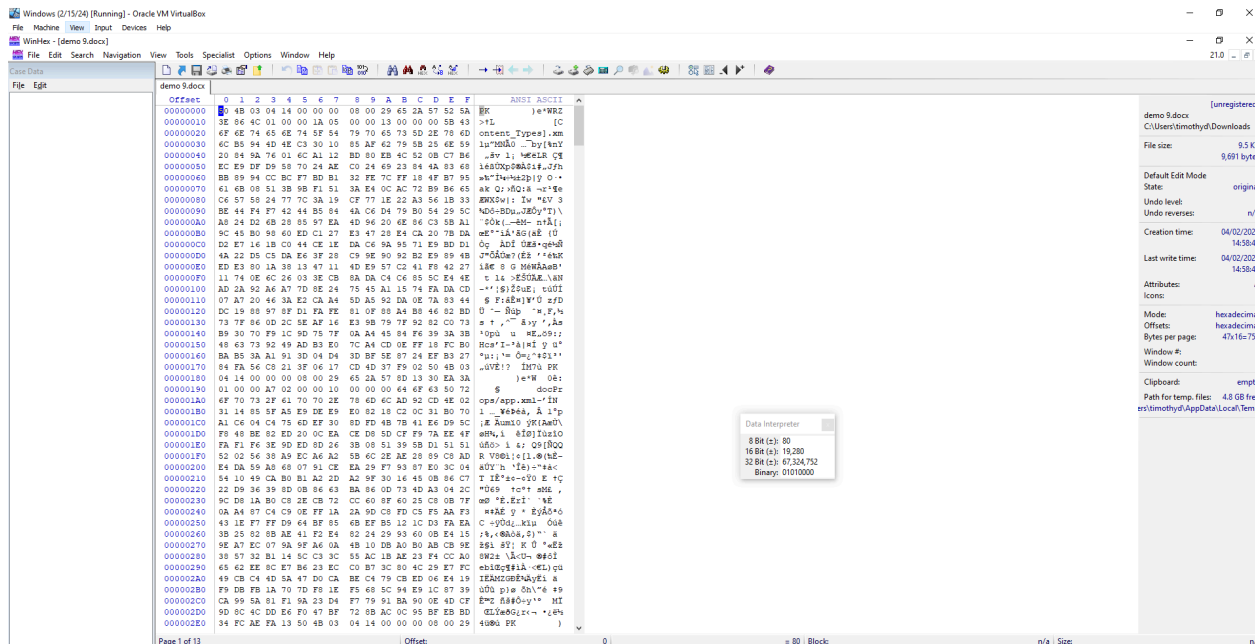


After rerunning the module, we can see that the hash set hits includes the identified images from the md5 hash.

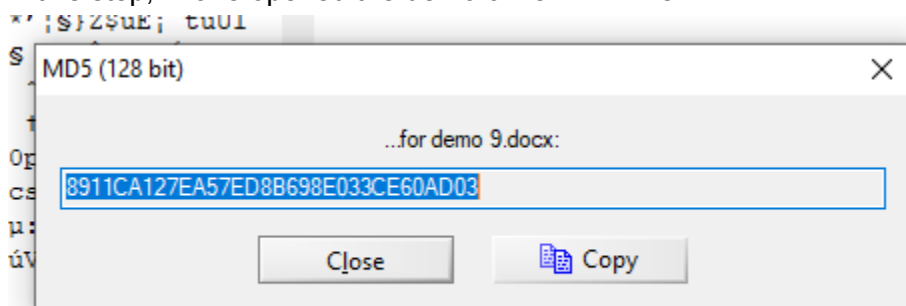
Task 2:



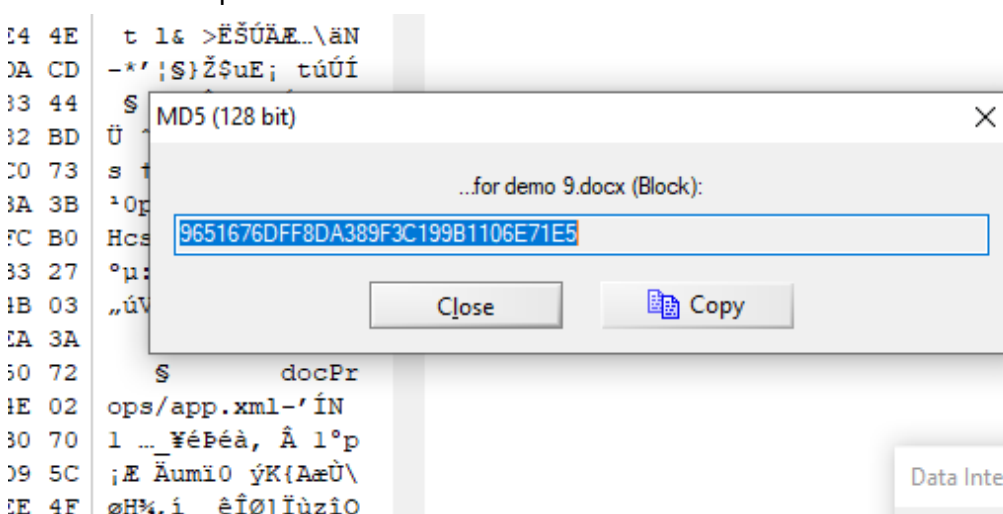
WinHex has been downloaded on my Windows VM.



In this step, I have opened the demo 9 file in WinHex.

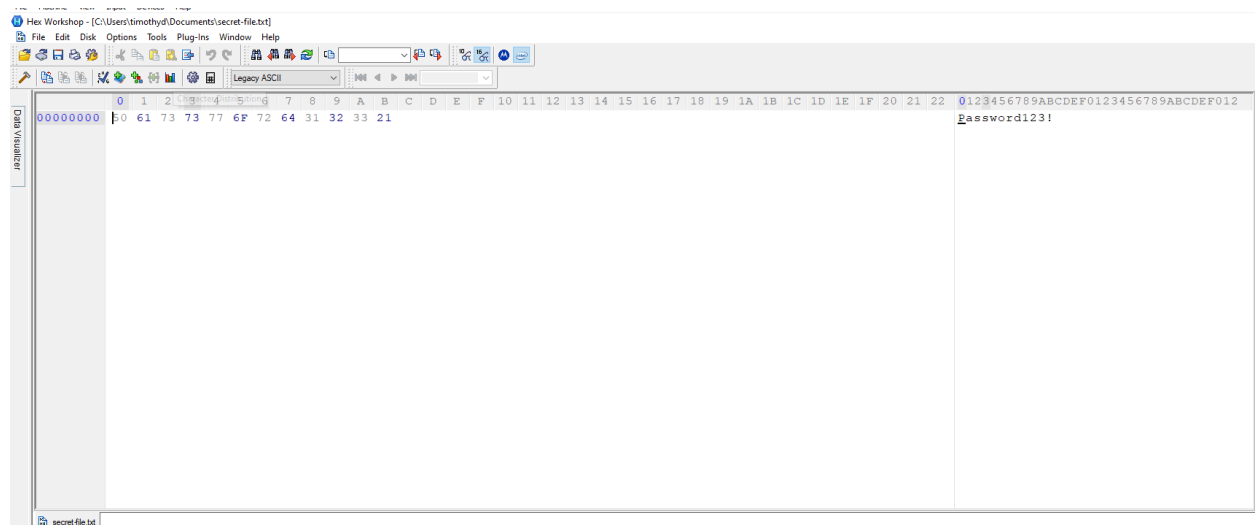


Here I have computed the hash.

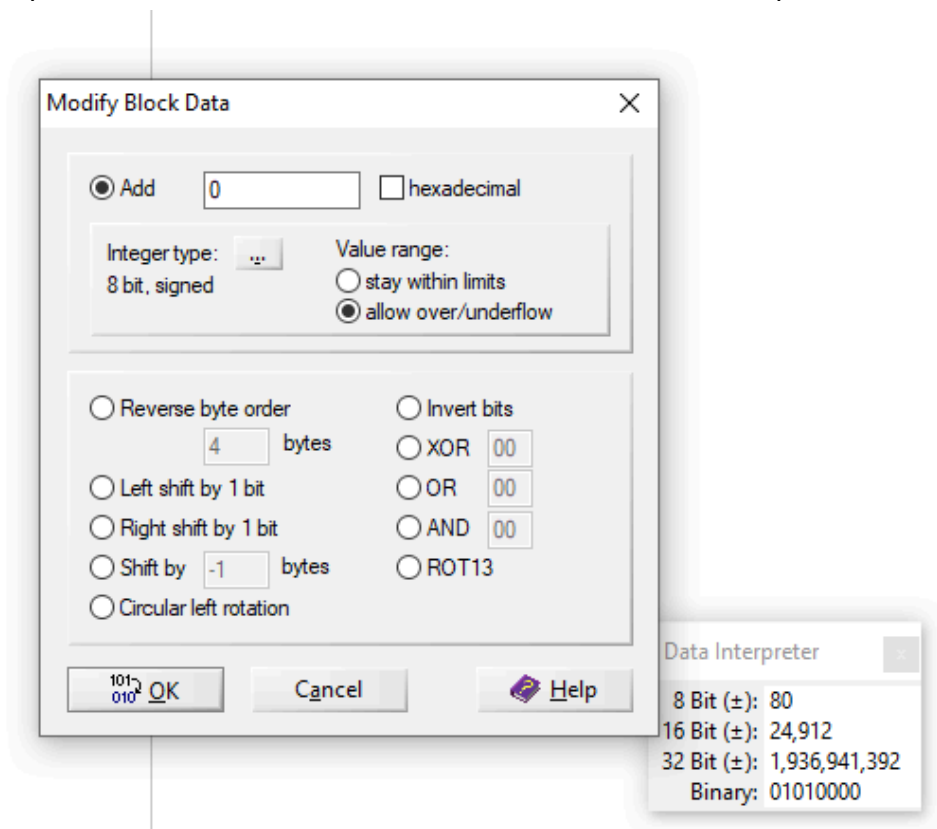


After selecting the first 16 bytes, we can see that the hash is different from the previous step.

Task 3:



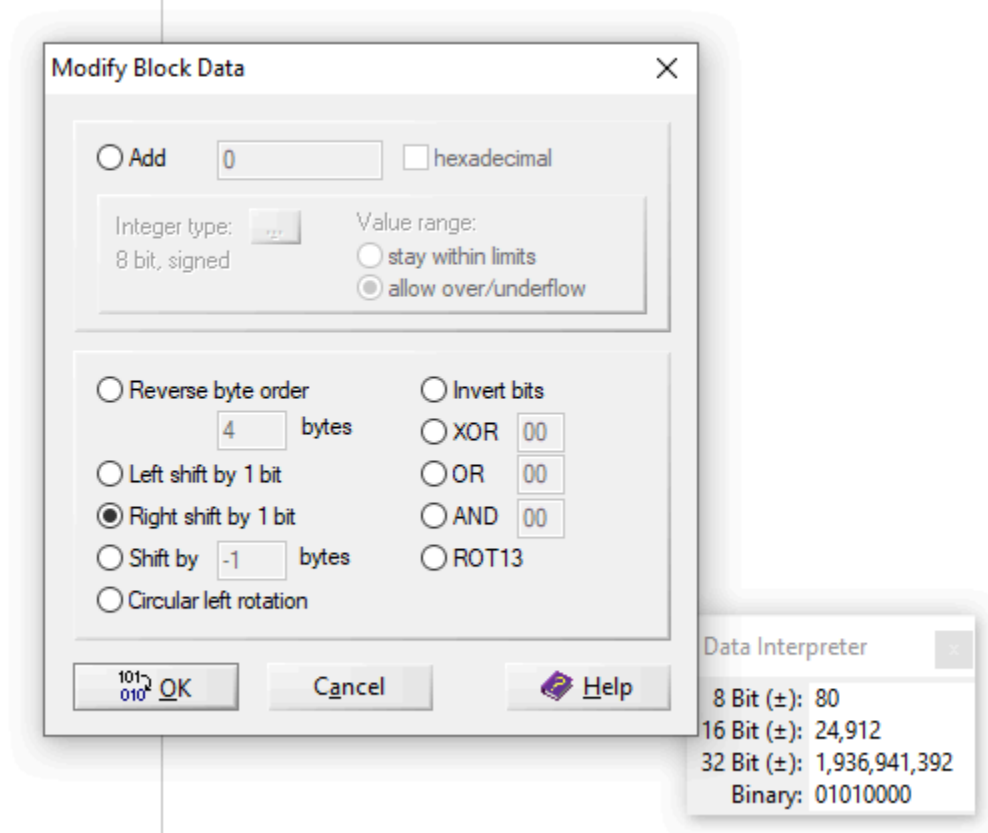
In this step, I have created a file with some text in it. I then have it opened in WinHex.



In this step, I have highlighted all the data and am going to modify it.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	20	C2	E6	E6	EE	DE	E4	C8	62	64	66	42					ÀæïþàÉbdfB

Here we can see the data has been altered.



In this step, I am modifying the data by doing a right shift by 1.

VXWINEX - [SECRET-FILE.TXT]

File Edit Search Navigation View Tools Specialist Options Window Help

Case Data

File Edit

secret-file.txt

Offset

00000000

0123456789A B C D E F

50 61 73 73 77 6F 72 64 31 32 33 20

ANSI ASCII

Password123

Here we can see the data is recovered.