Worcester Polytechnic Institute
Department of Computer Science

Activity 5.5: Recovering Graphics Files

Objectives:

- Split and combine files in Linux.
- Use WinHex to recover graphics files.

Instructions:

Part 1: Split and combine files in Linux.

Since Winhex evaluation version cannot process a file that is bigger than 200KB, you need to split a file to pieces in order to edit and save a big file.

1. Download the file "funpicture" from Canvas onto a Linux machine (your local Linux machine or the CAINE/Kali virtual machine, Mac OS also works).
2. Open terminal in Linux and change to the directory that contains funpicture.
3. Split the file "funpicture" by typing command:
   split –b 19000 funpicture

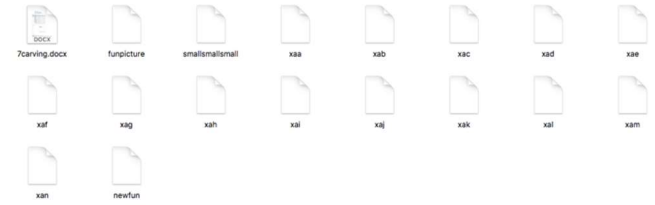
```
[YUCCA:hands-on activities/instructions/7carving] sun% ls
7carving.docx   funpicture      smallsmallsmall ~$arving.docx
[YUCCA:hands-on activities/instructions/7carving] sun% split -b 190
000 funpicture
```

4. Type command **ls** to see the file pieces.

```
[YUCCA:hands-on activities/instructions/7carving] sun% ls
7carving.docx   xac             xah             xam
funpicture      xad             xai             xan
smallsmallsmall xae             xaj             ~$arving.docx
xaa             xaf             xak
xab             xag             xal
```

5. Combine the file pieces to a new file by typing command:
   cat x*>newfun

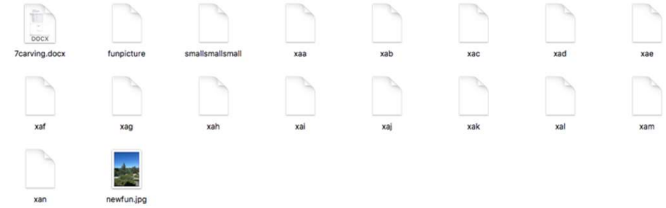
```
[YUCCA:hands-on activities/instructions/7carving] sun% cat x*>newfun
[YUCCA:hands-on activities/instructions/7carving] sun% ls
7carving.docx   xab             xag             xal
funpicture      xac             xah             xam
newfun          xad             xai             xan
smallsmallsmall xae             xaj             ~$arving.docx
xaa             xaf             xak
```



6. Rename the newfun file to newfun.jpg by typing command:

```
sun% mv newfun newfun.jpg
```

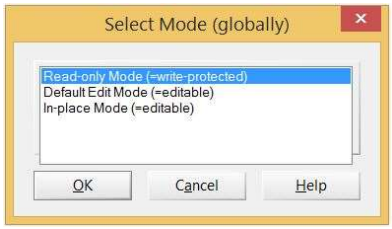
7. Click on the newfun.jpg file to display it.



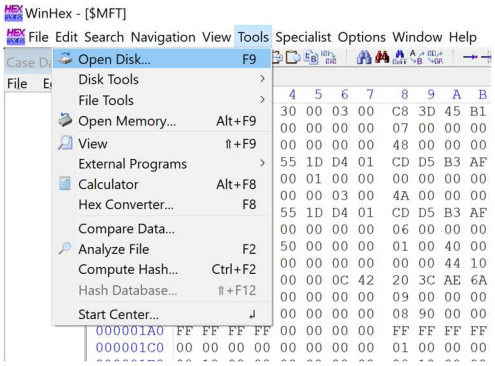
8. Or you can combine the steps 5-6 into one step by tying command:
   cat x*>newfun.jpg

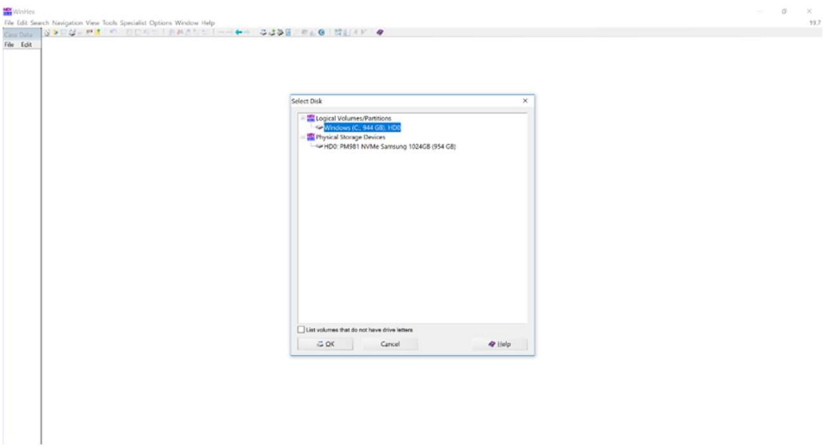
Part 2: Practice recovering graphics files using Winhex.

9. Download file “smallsmallsmall” from Canvas and save it to a folder. This file is a PNG file, but the header has been modified by the suspect.
10. Start WinHex with the **Run as administrator** option. If you see an evaluation warning message, click **OK**.
    As a safety precaution, click **Options**, **Edit Mode** from the menu. In the Select Mode dialog box, click **Read-Only Mode** (=**write protected**), as shown in Figure 2, and then click **OK**.



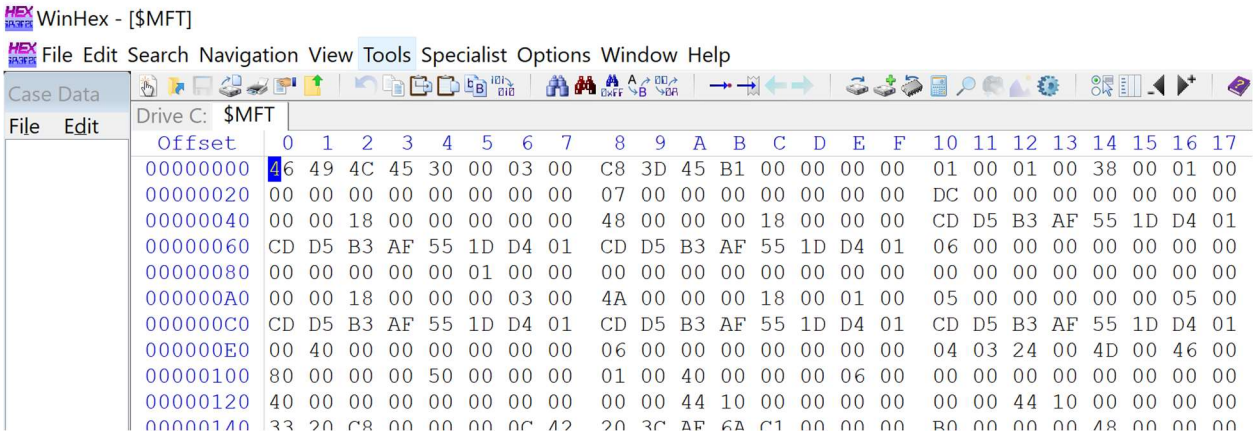
11. Click **Tools**, **Open Disk** from the menu. In the **View Disk** dialog box, click the drive where you saved smallsmallsmall, and then click **OK**. If you’re prompted to take a new snapshot, click **Take a new one**. Depending on the size and quantity of data on your disk, it might take several minutes for WinHex to traverse all the files and paths on your disk drive.





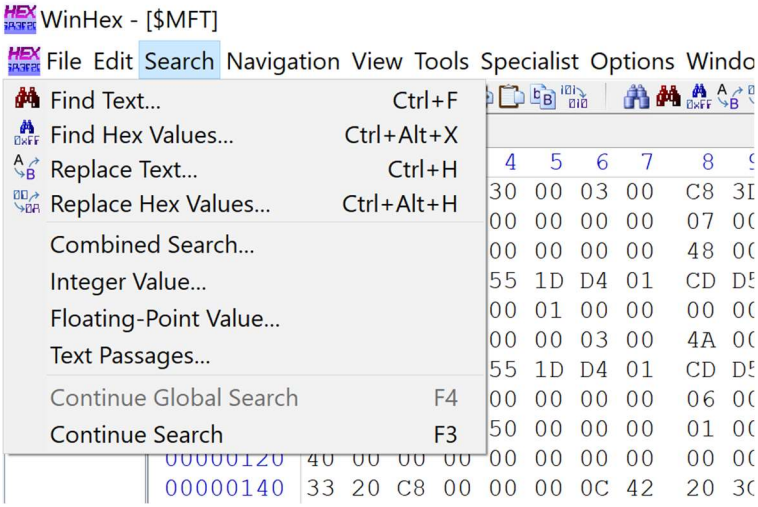
The following steps will find the file “smallsmallsmall” and recover it. Of course, in this lab, you can directly navigate to your work folder where smallsmallsmall file is stored and work on that. However, in a real investigation, you may not know where the file was stored. You can then do a search in the $MFT to find it.

12. Scroll down and find the $MFT file, right click and choose “open”. You’ll open the MFT file in a new window.

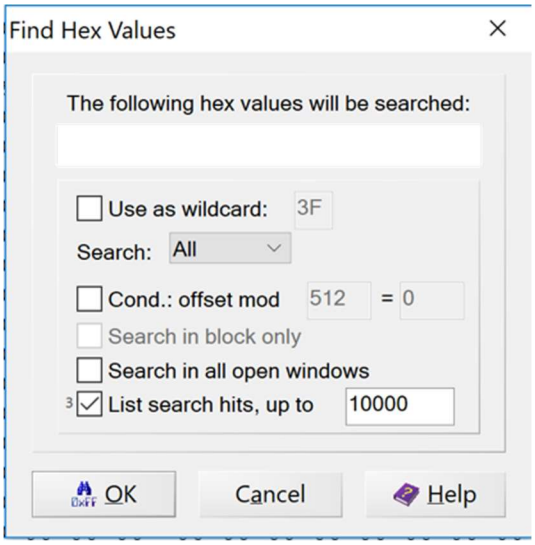


Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10	11	12	13	14	15	16	17
00000000	46	49	4C	45	30	00	03	00	C8	3D	45	B1	00	00	00	00	01	00	01	00	38	00	01	00
00000020	00	00	00	00	00	00	00	00	07	00	00	00	00	00	00	00	DC	00	00	00	00	00	00	00
00000040	00	00	18	00	00	00	00	00	48	00	00	00	18	00	00	00	CD	D5	B3	AF	55	1D	D4	01
00000060	CD	D5	B3	AF	55	1D	D4	01	CD	D5	B3	AF	55	1D	D4	01	06	00	00	00	00	00	00	00
00000080	00	00	00	00	00	01	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000A0	00	00	18	00	00	00	03	00	4A	00	00	00	18	00	01	00	05	00	00	00	00	00	05	00
000000C0	CD	D5	B3	AF	55	1D	D4	01	CD	D5	B3	AF	55	1D	D4	01	CD	D5	B3	AF	55	1D	D4	01
000000E0	00	40	00	00	00	00	00	00	06	00	00	00	00	00	00	00	04	03	24	00	4D	00	46	00
00000100	80	00	00	00	50	00	00	00	01	00	40	00	00	00	06	00	00	00	00	00	00	00	00	00
00000120	40	00	00	00	00	00	00	00	00	00	44	10	00	00	00	00	00	00	44	10	00	00	00	00
00000140	33	20	C8	00	00	00	0C	42	20	3C	AF	6A	C1	00	00	00	B0	00	00	00	48	00	00	00

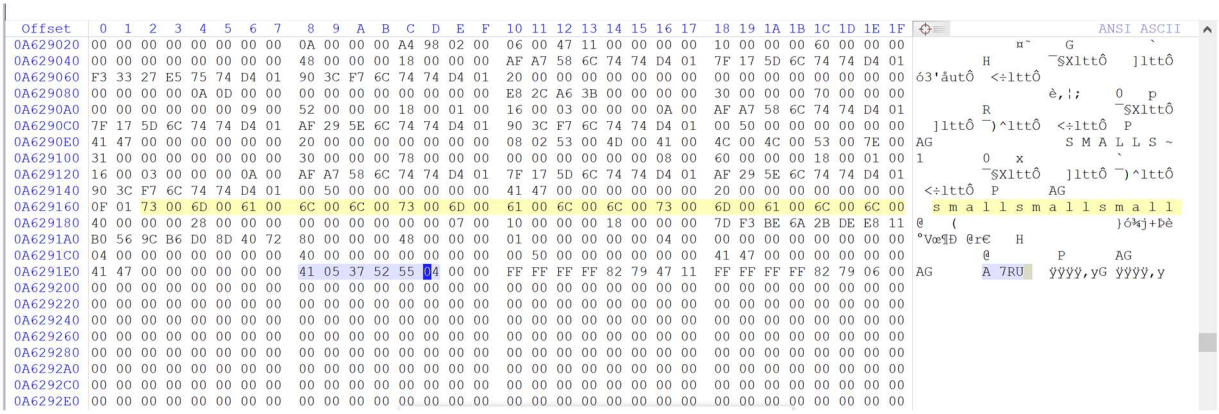
13. The next task is to find the “smallsmallsmall” file. In $MFT, the characters in a file name are usually separated by hexadecimal value “00”. For example, if the file name is “ab”, then it appears in the $MFT as “61006200”. 61 is the hexadecimal value for letter “a”, and 62 is the hexadecimal for letter “b”. Please google search the hexadecimal values for “smallsmallsmall” and write them down. Prepare the hexadecimal values that should appear as the file name for “smallsmallsmall” file.
14. Click on Search, then Find Hex Values.



15. Type in the hexadecimal values for “smallsmallsmall” file name that you’ve prepared in step 13.

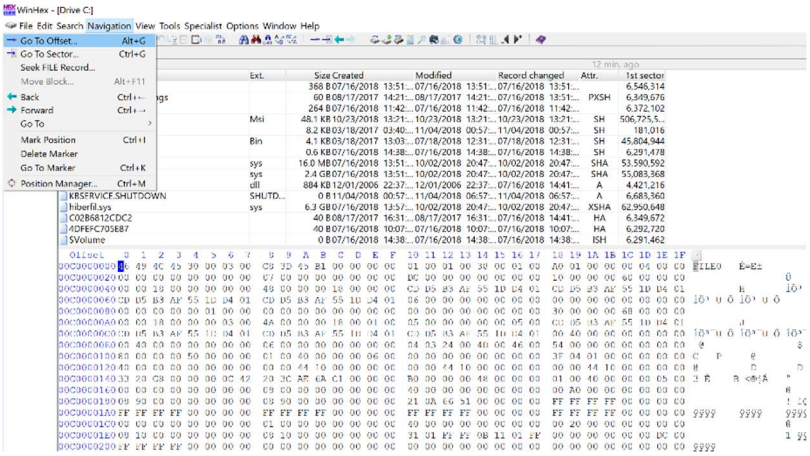


16. You will find a hit after the search.

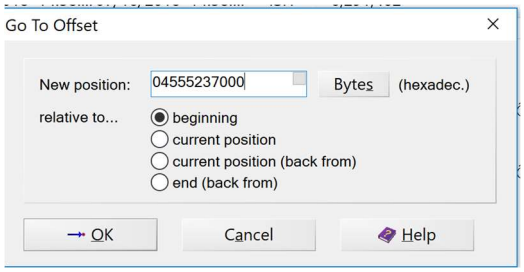


17. Please follow the same methodology as in hands-on activity 5 and lab 2 to examine this $MFT file record. You need to find out the dataruns for this file. In the demo, the first datarun information is “41 05 37 52 55 04”. This means the starting position of the first datarun is “0x 04 55 52 37” and the size is “0x05”.

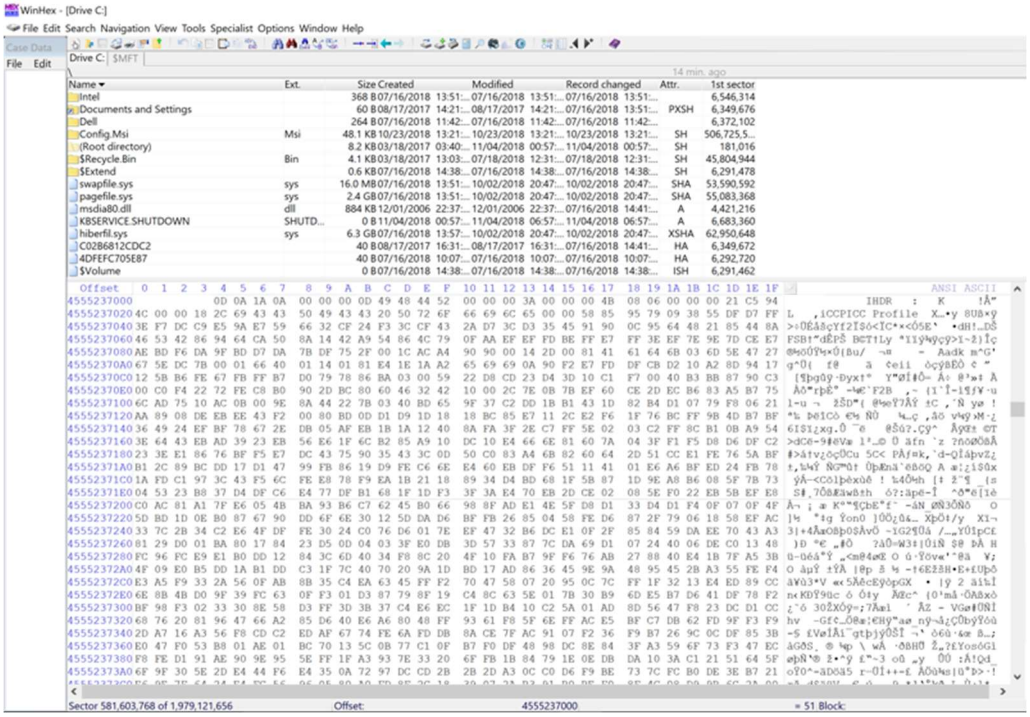
18. ***Open the window for the entire disk (Drive C: in my case).*** Click on **Navigation**, and then click on **Go To Offset**. Pay attention: you need to do “Go To Offset” on the “Drive C” tab, not the MFT tab, because the offset position you found is the position on the Drive, not in the MFT file.



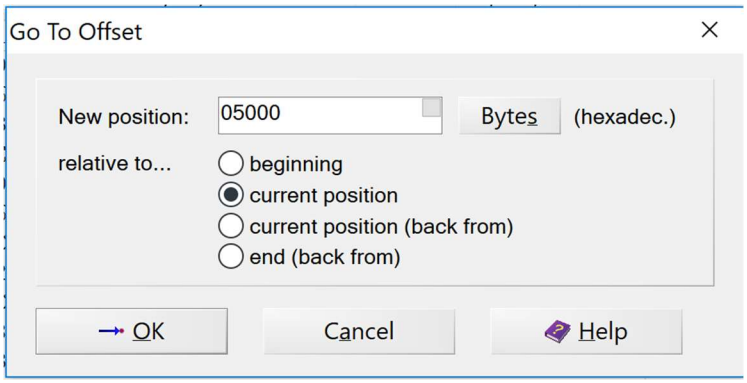
19. Type in the starting position of the first data run in big endian and choose **beginning**, then click on **OK**. In this demo, it is the value of “04 55 52 37” appended with three 0s.



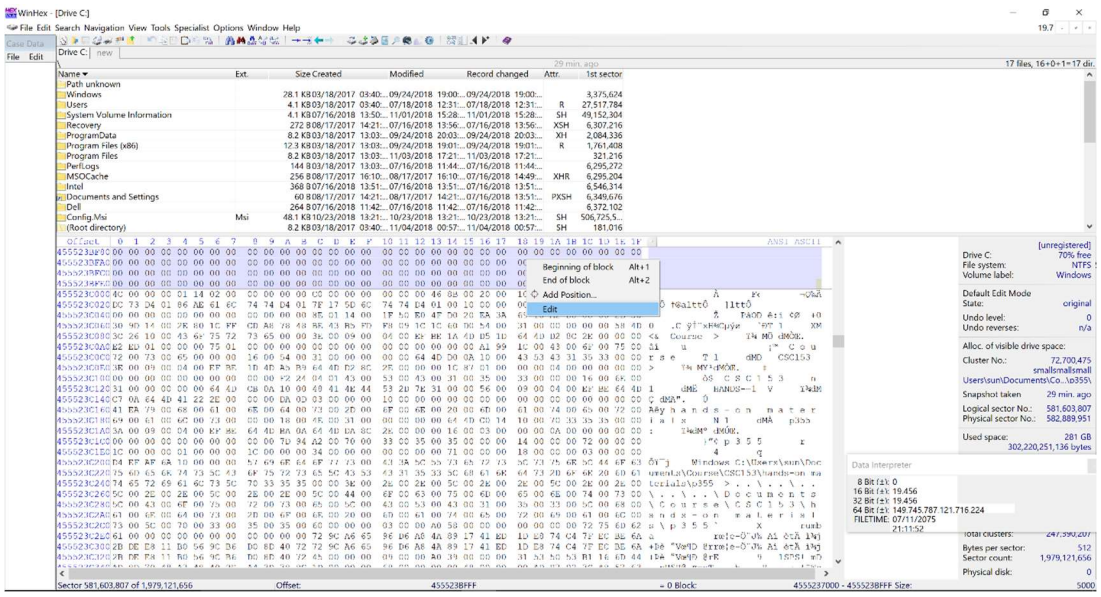
20. This will guide you to the beginning of the “smallsmallsmall” file.

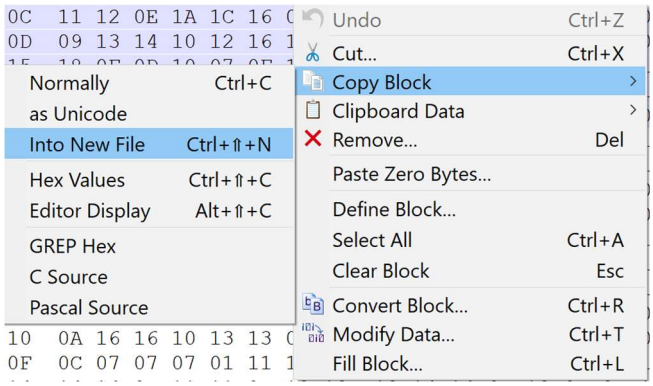


21. Since the size of the first datarun is “05”, you may click on **Navigation**, and then click on **Go To Offset** again to find the end of the first datarun**.**
22. Type in **05000** in the position and choose **current position**. Click on OK. The ending position for the first datarun in this demo is 0x 45 55 23 C0 00.

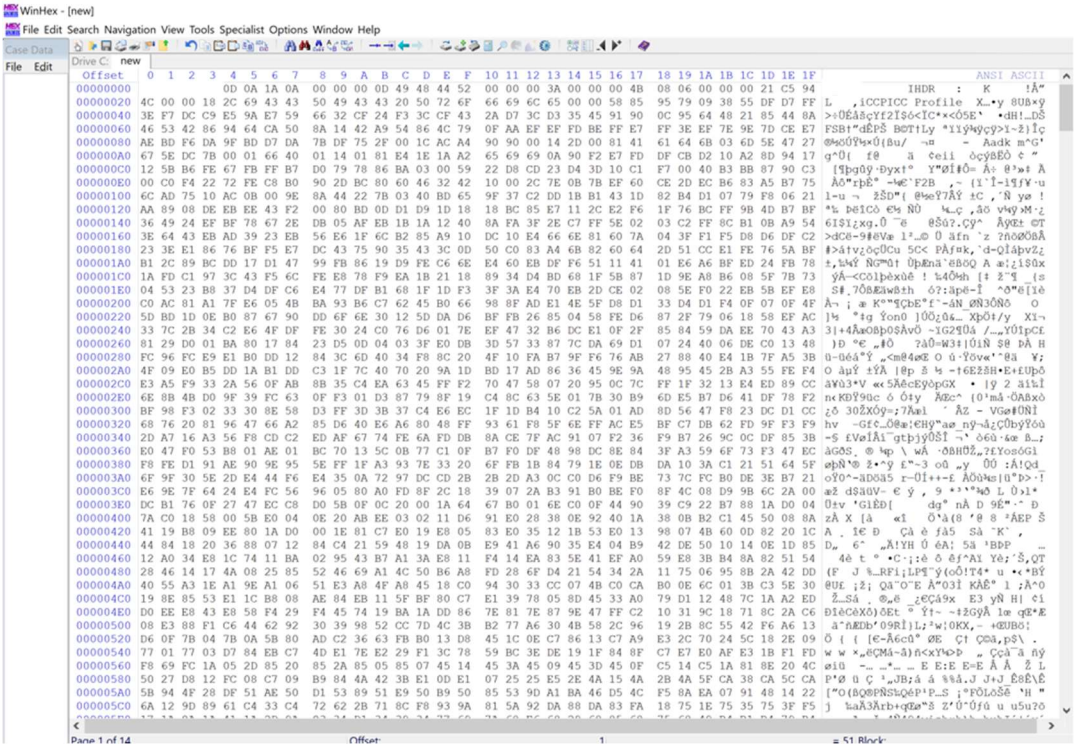


23. Go back to the beginning of the file again using go to offset. Click on the first byte of the file and drag it until the offset is “5000” (you need to replace the offset with your own number), which is the size of the first datarun. Right click and choose **Edit**, then choose **Copy Block**, then choose **Into New File**. Type in the file name as “**new**” and click on **Save**.





24. Google search the correct header for PNG file format, and change the header of the **new** file to the correct format.



25. (You may skip this step if you only have one data run.) If you have more than 1 data runs, you need to follow the same method as in Step 19-23 to copy the data in other data runs and append that into "**new**" file. Pay attention to the following things:
    a. The starting position for the second data run is a relative position from the starting position of the first data run, so you should choose from "current position" when repeating step 19;
    b. Instead of copying all data runs into the "new" file, a safer way is to first save the data runs in separate files, and then combine these files into one file.
26. After the header is changed, click on **File**, and then **Save As**, type in "**recovered**" as the file name.
27. Find the "recovered" file, and add the extension of "png".

Questions:

1. What the hexadecimal values did you use to search for the file "smallsmallsmall" in step 13 and 15?
2. Is the file a resident file or non-resident file? How do you know? Please take a screenshot to show the evidence.
3. How many data runs does this file has? Please take a screenshot to show the evidence.
4. What is the starting position for the first data run? Please take a screenshot to show the evidence.
5. What is the size of the first data run?
6. In step 20, what is the header of the file "smallsmallsmall" which you downloaded from Canvas? Please provide the first 4 bytes of the hexadecimal values. Please take a screenshot to show the evidence.
7. What should be the correct header of a PNG file?
8. Take a screenshot to show the recovered file.
9. Compared to Foremost, Scalpel, what is the advantage to carve file manually?

Deliverable:

Note: You need to submit a lab report to Canvas. Your lab report should **contain two sections.**

1. In section 1, you should document the most important steps in this hands-on activity. Please include **necessary narrative and analysis** to make your report clear. Take ***at least 5*** screenshots to document the steps.
2. In section 2, you should answer the questions above. **Answer questions using big endian. Answer questions using Hexadecimal when necessary.** Your lab report should ***explicitly*** **answer all questions one by one**. When necessary, you need to have screenshots to prove your answer (These screenshots are additional to the screenshots in section 1 of the report). The report will be evaluated based on the correctness, completeness, clarity and quality of English writing.