Worcester Polytechnic Institute
Department of Computer Science

Lab 5-Module 5.2: Foremost

Objectives

- File carving using Foremost

Task

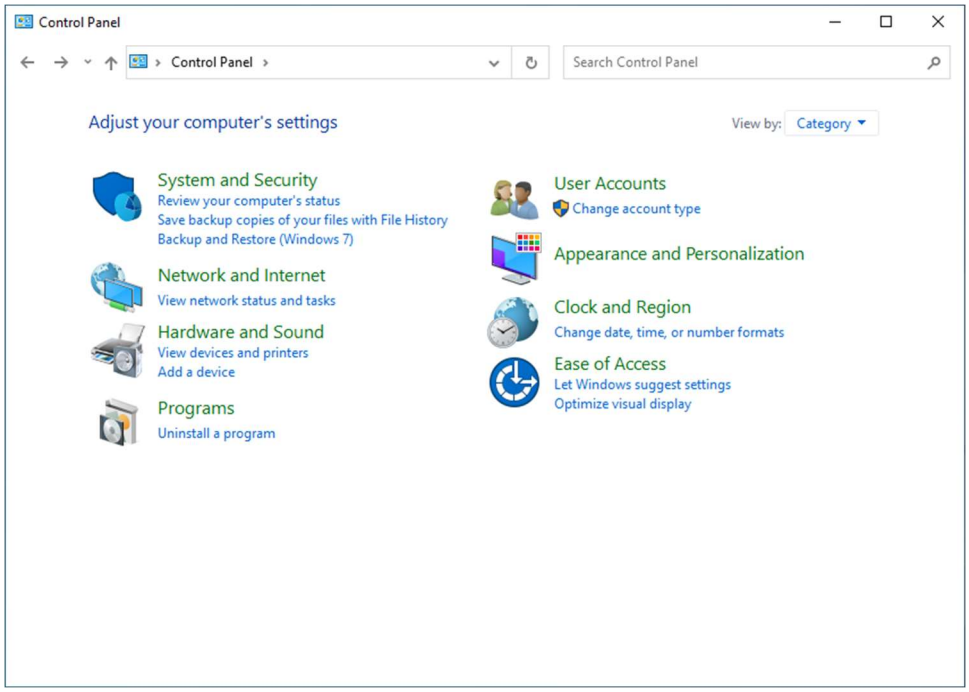
Task 1. Software Preparation

1. In a window system (can be a VM), download the folder “m5” onto the desktop.

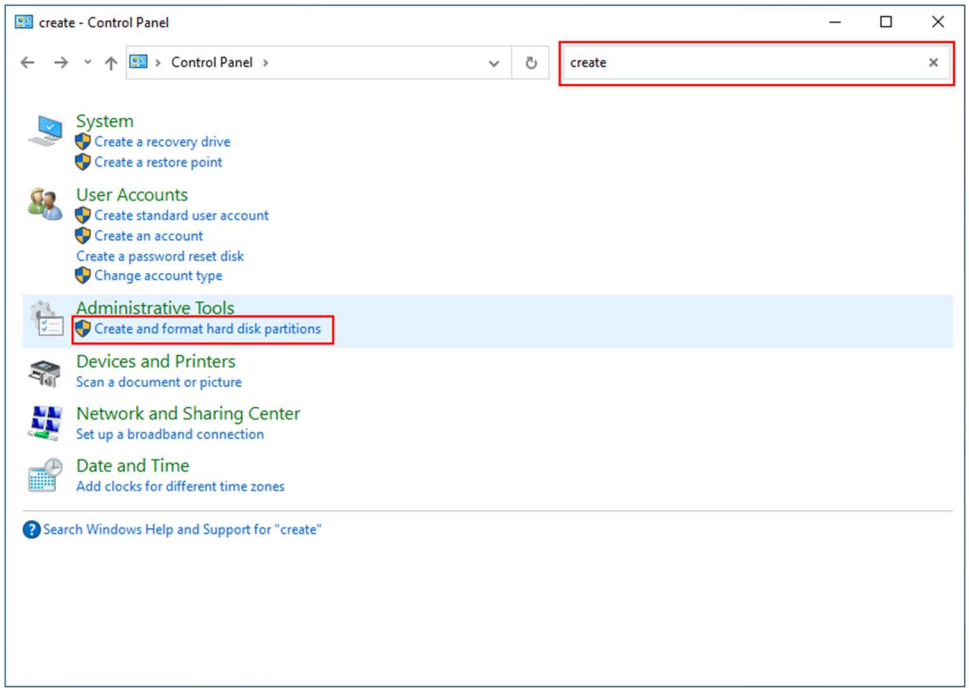
Folder m5 download link:
https://drive.google.com/drive/folders/1sUTNOxCAuNT46EsJnrxWO2Nyy9C6C5Ep?usp=sharing

Task 2. Create an “empty” disk partition

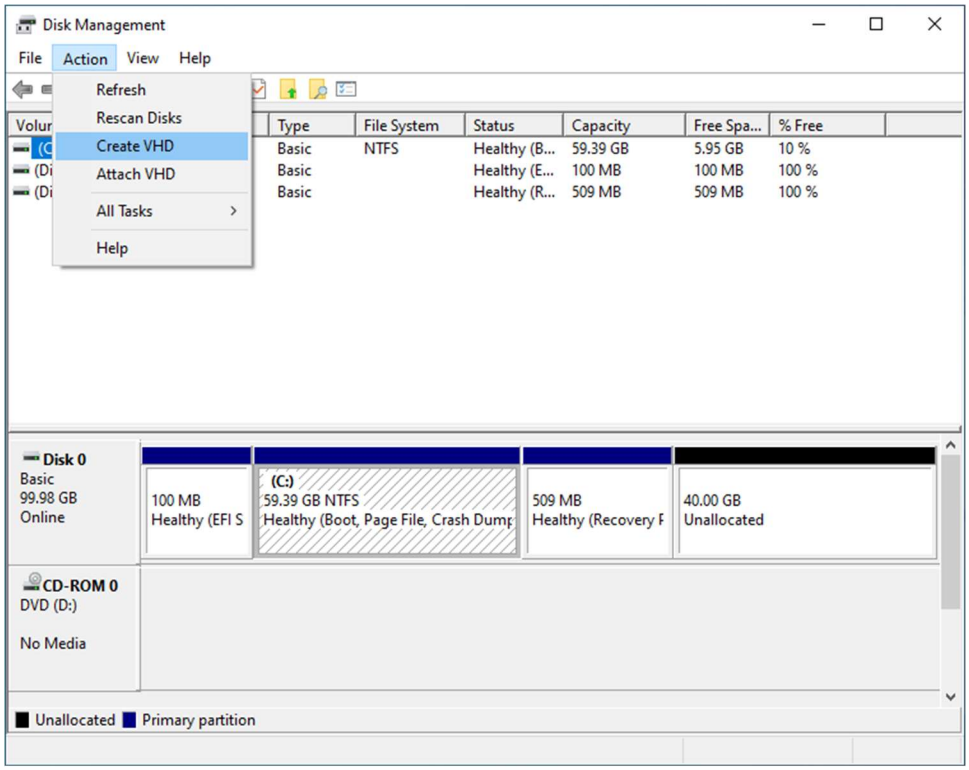
1. In Window system, open the control panel.

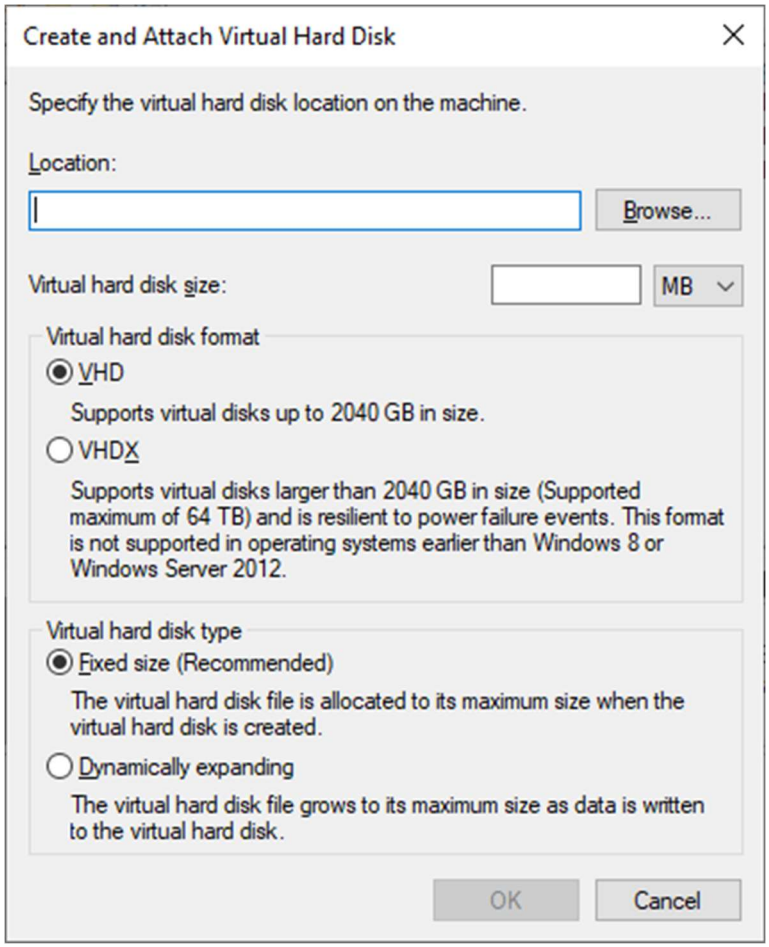


2. Then, on the top right, search for “create and format hard disk partitions” and open the disk management.

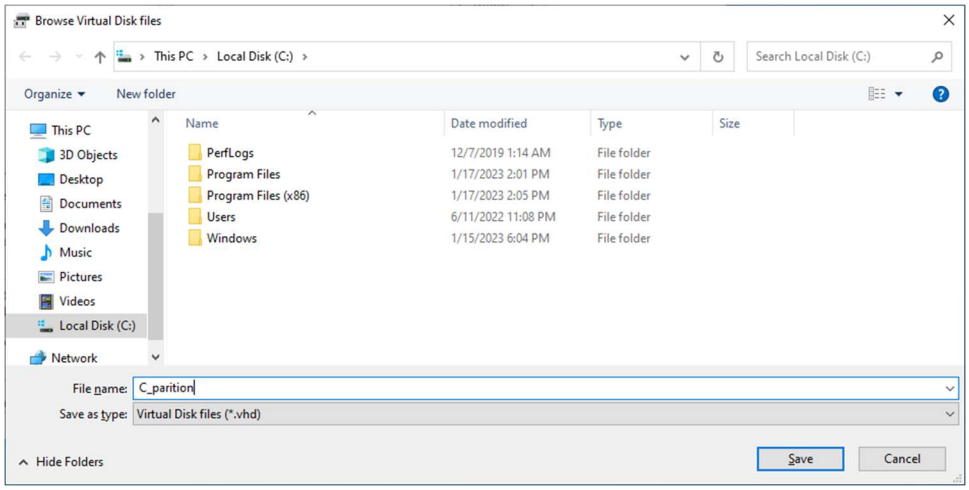


3. Select “Action”-> “Create VHD”

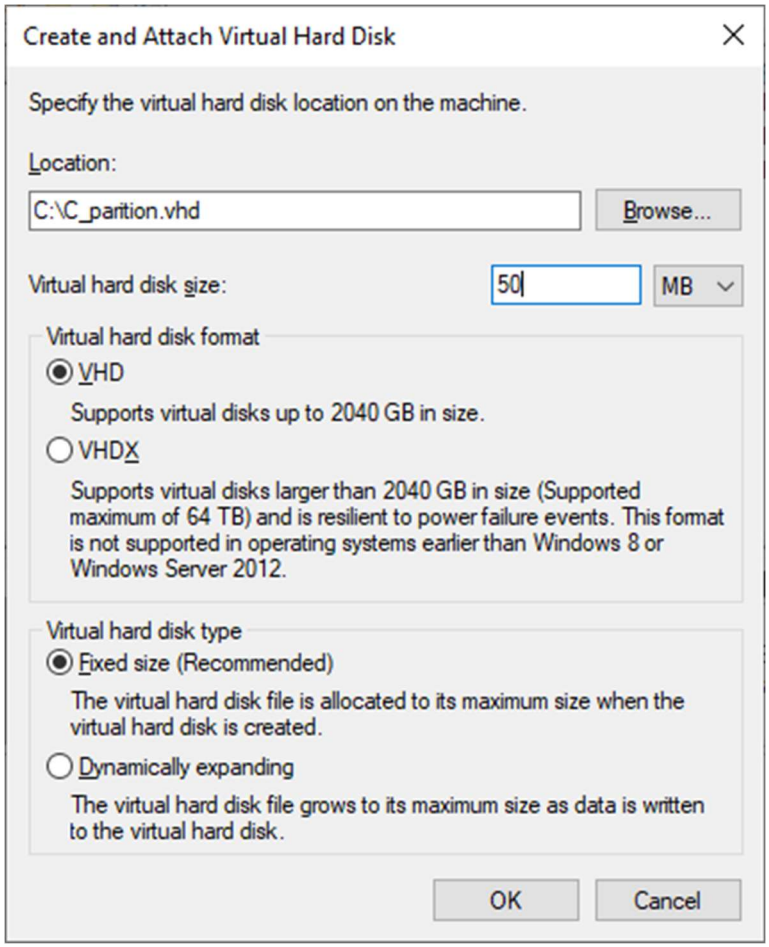




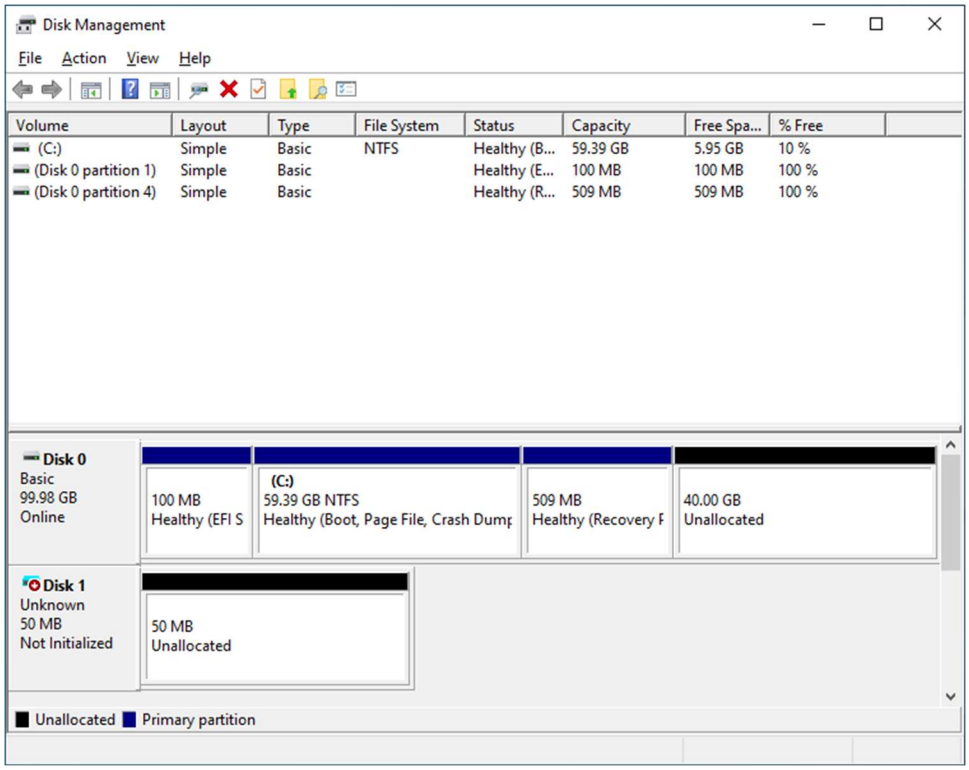
4. For the location, click on “Browse” and select C: and named it “C_partition”, click save.



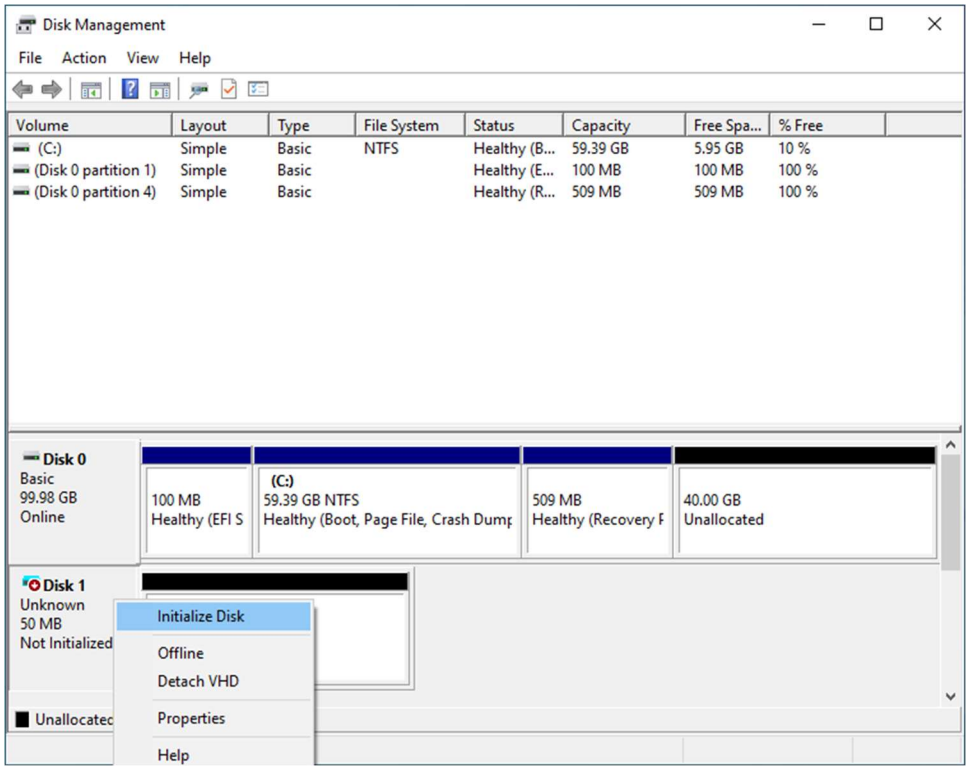
5. Then, enter 50 MB for the virtual hard disk size and leave the other settings as default, click OK.



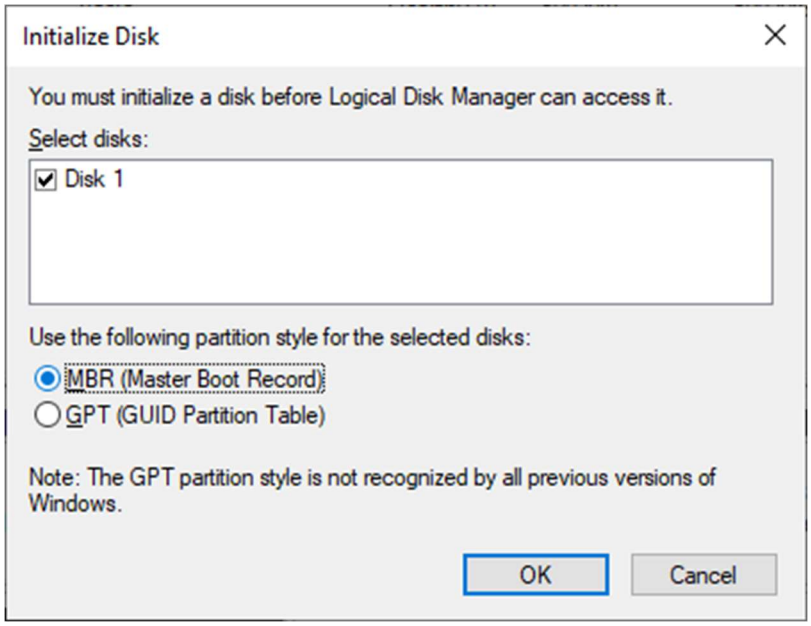
(You should then see a new disk being created, and a red mark on its icon.)



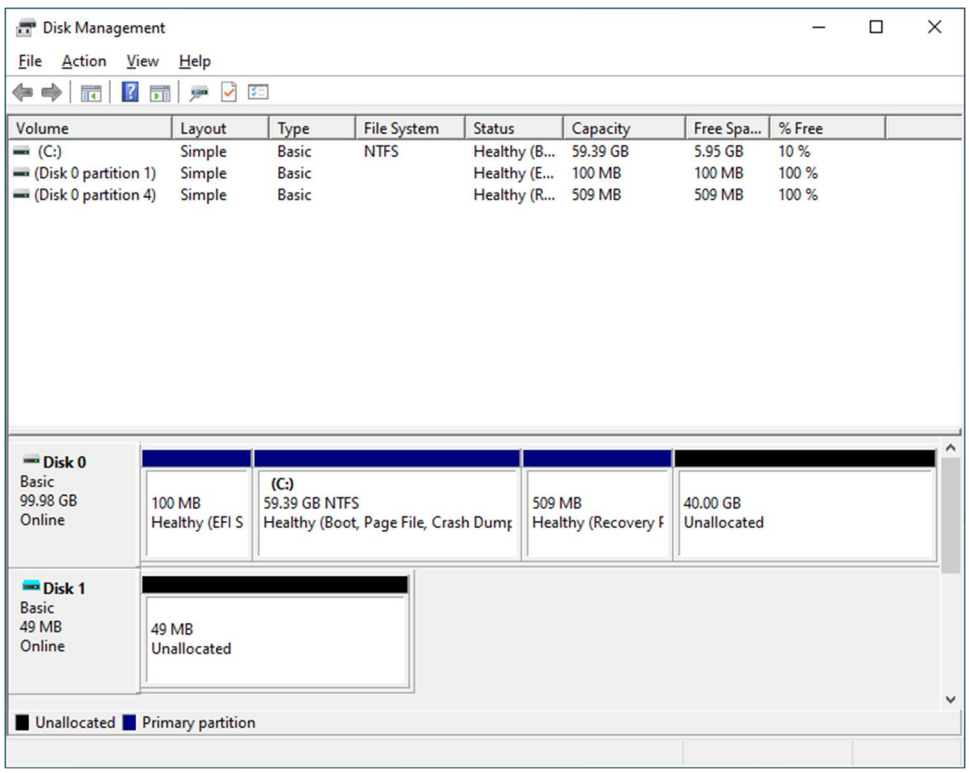
6. Right click on of disk and select “Initialize Disk”



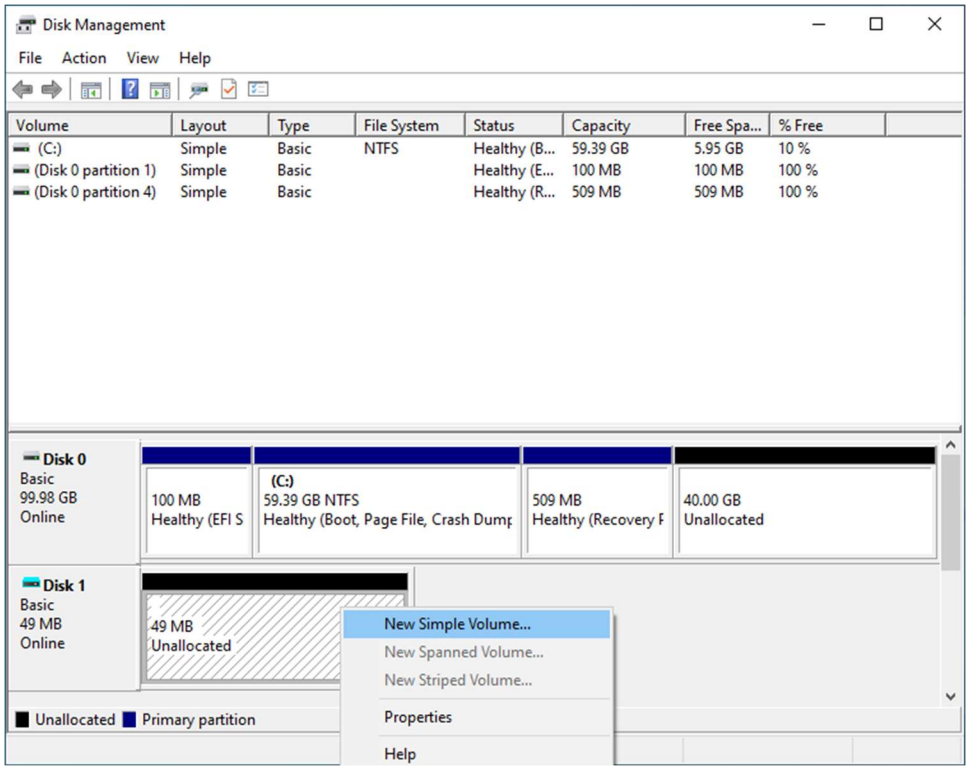
7. Change the partition style to MBR (Master Boot Record)



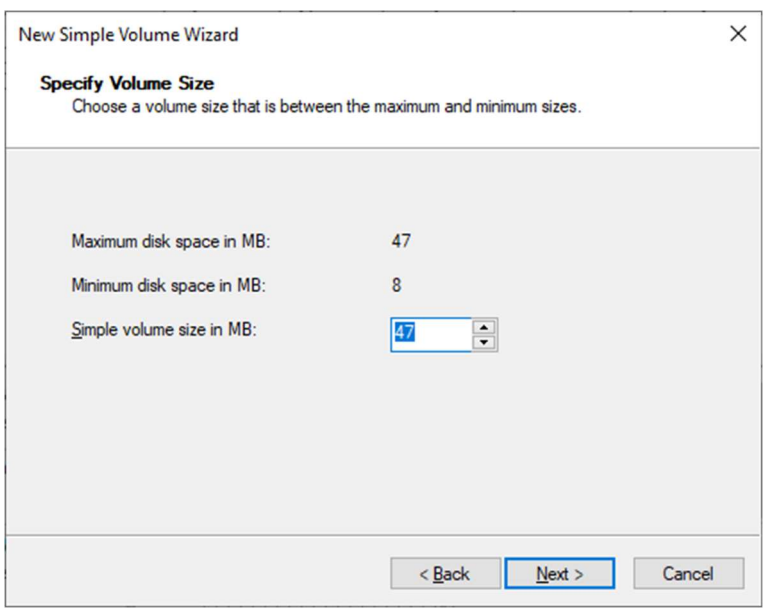
(You should now see the red mark icon is gone.)

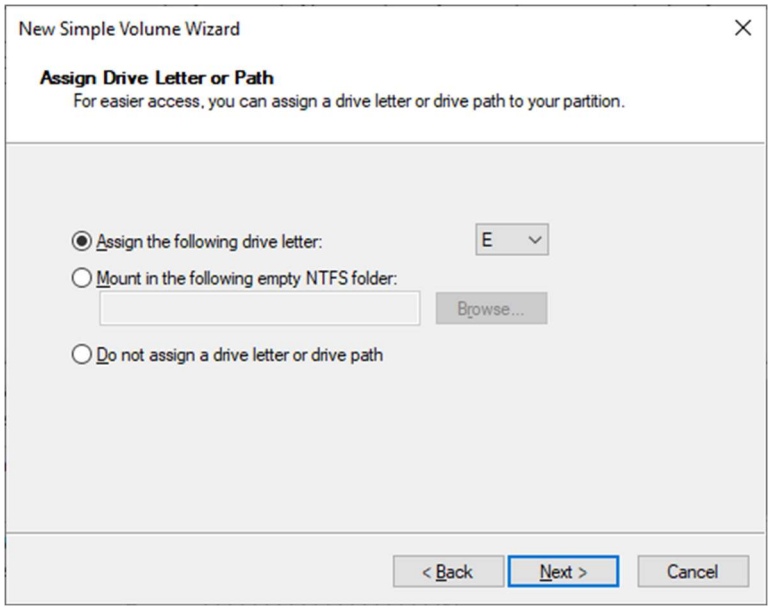


8. Right click on (right side of) disk and select “New Simple Volume...”

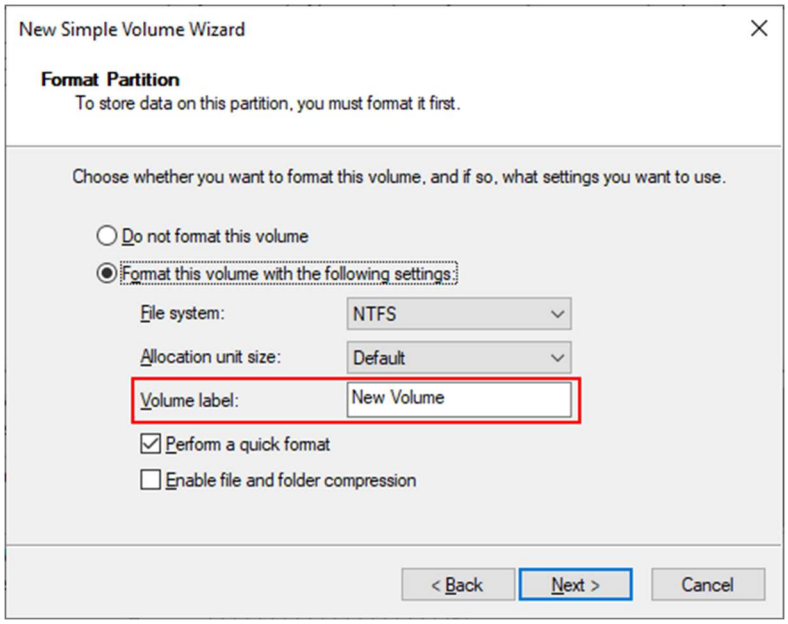


9. Follow the setup instruction and click “Next”, keep the default setting and click “Next”



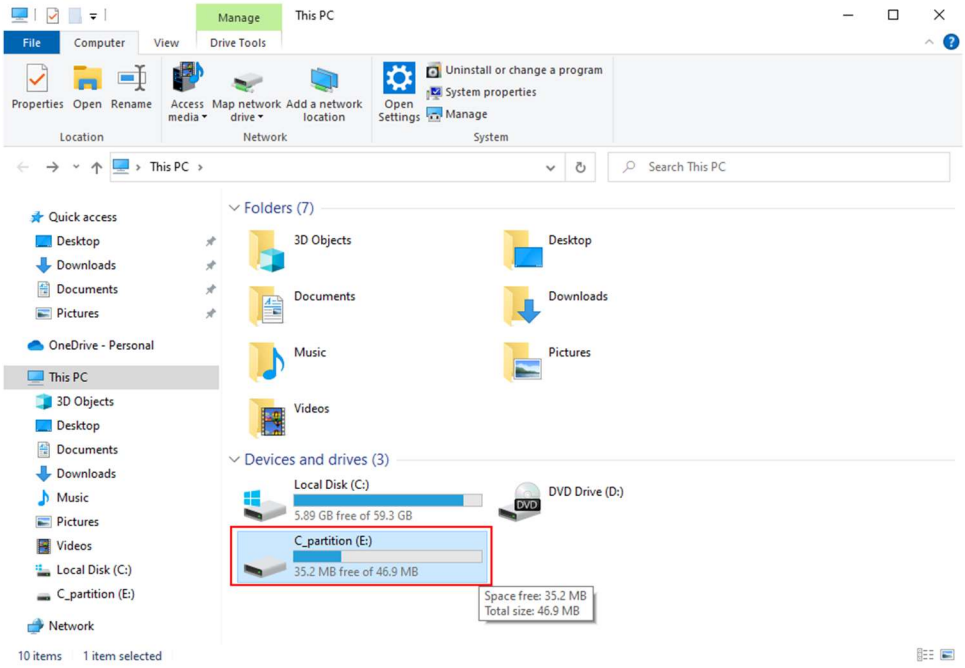


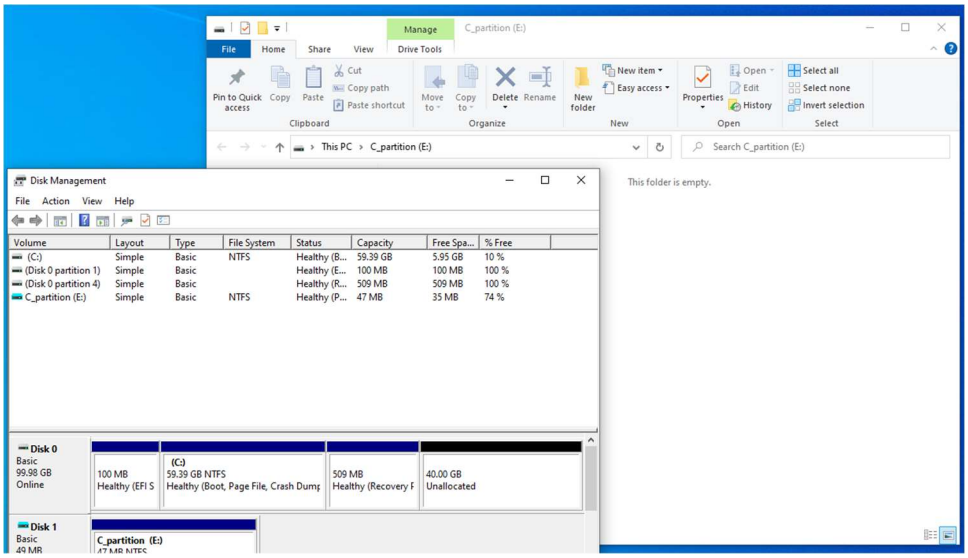
10. Rename the volume to “C_partition” under the Volume label. Then click “Next” and “Finish”.



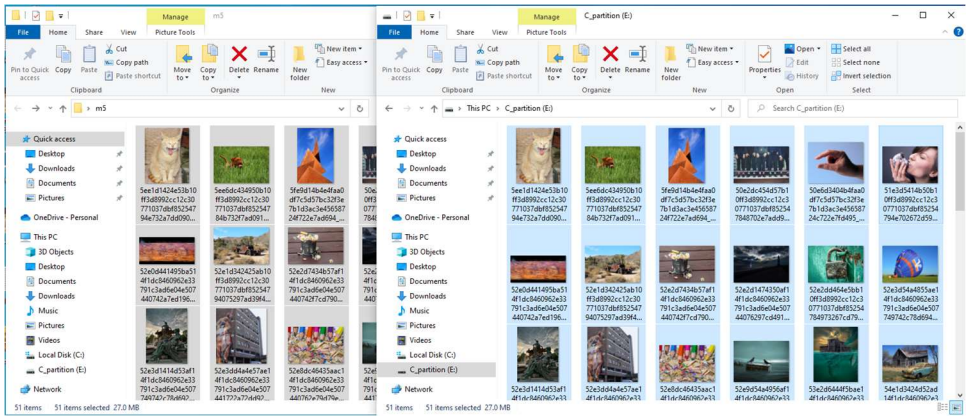
11. Windows should then automatically open the C_partition folder in the E: disk.

(If not, open the start menu and enter “this pc”)





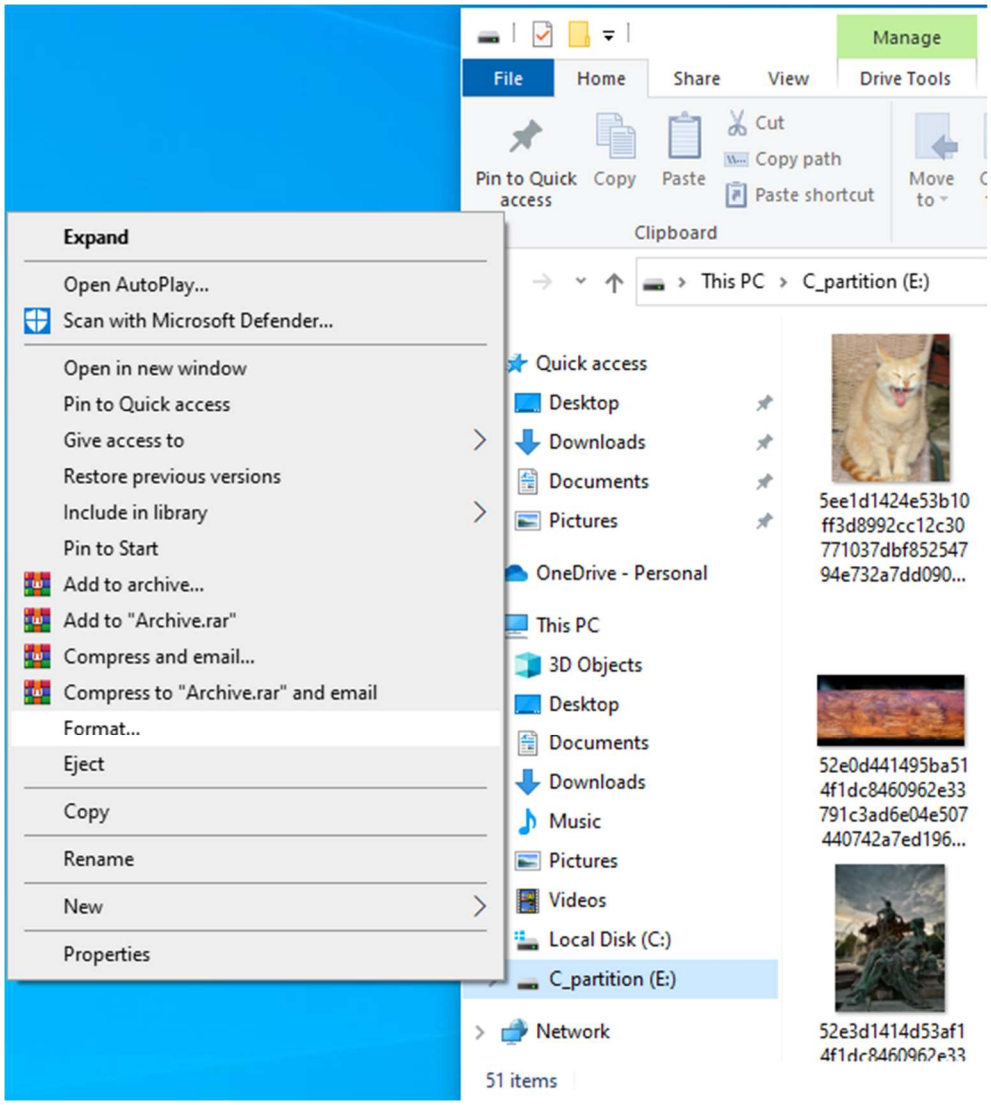
12. Copy all the files under the m5 folder onto the “C_partition” disk.



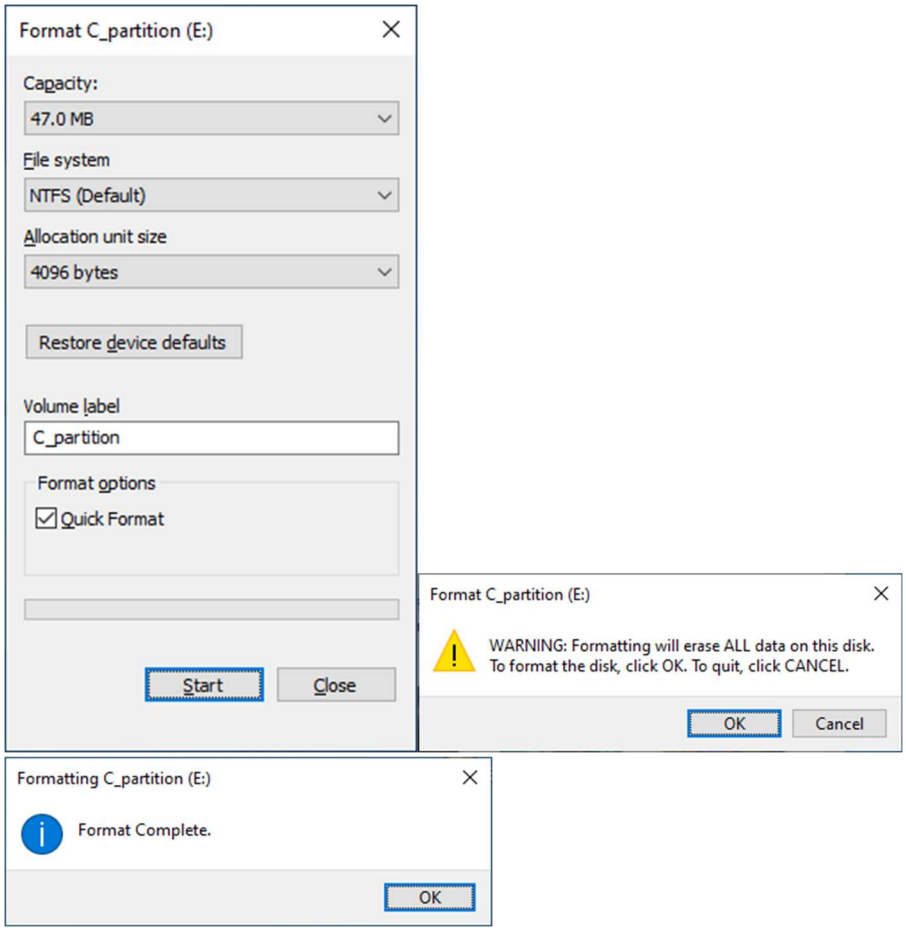
Now, we are going to delete and format the disk.

13. Right click the C_partition (E:) disk and select “Format”.

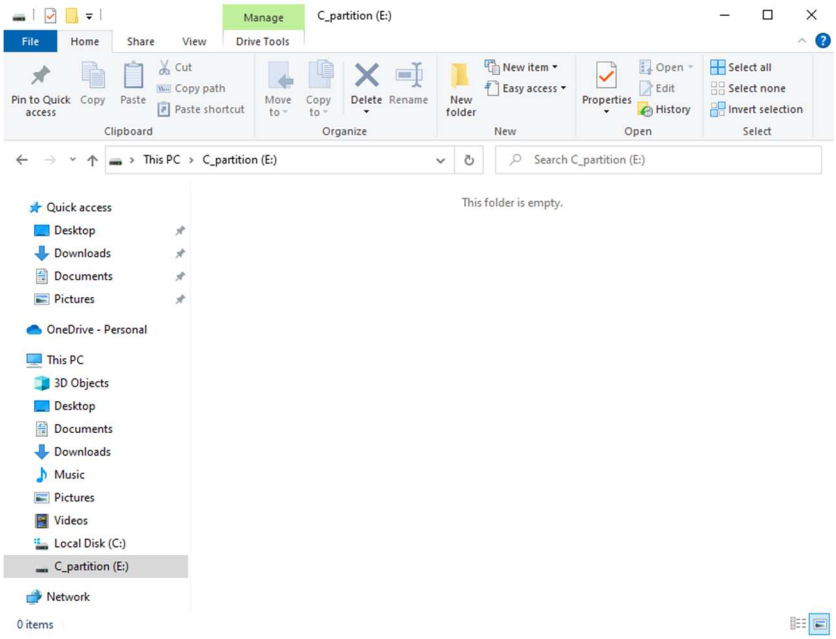
(* Make sure you have selected “C_partition” (E:) and not other disks ***)**



14. In the format setting, **make sure to check "Quick Format"** and leave other settings default. Then click "OK" for the warning message.

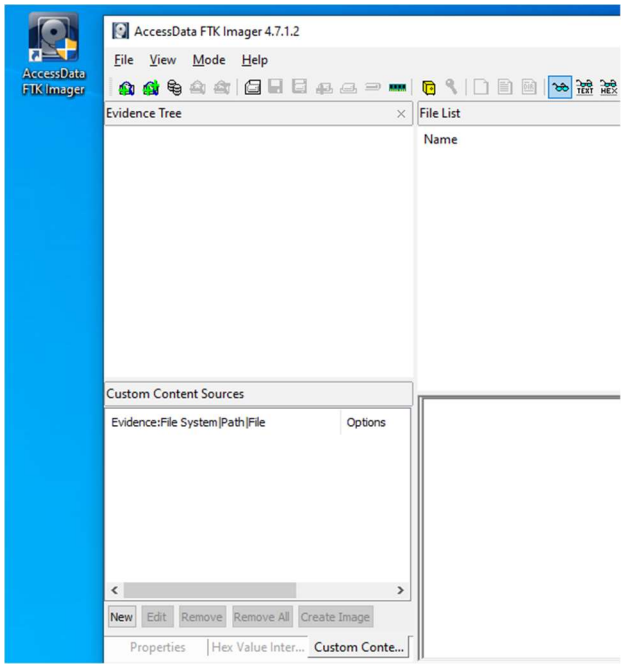


15. If you now go back to review the C_partiton (E:). Every file should be deleted.

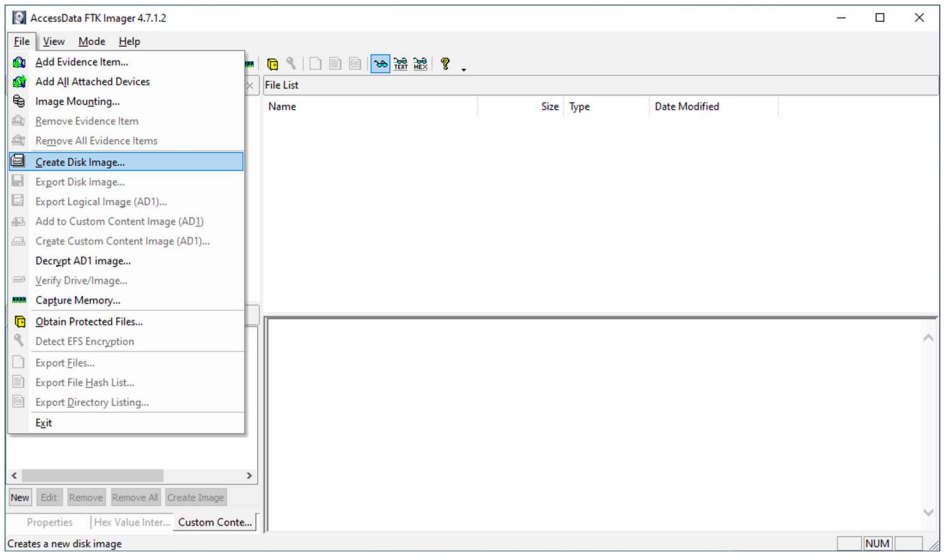


Task 3. Make an image of the “empty” disk with FTK Imager

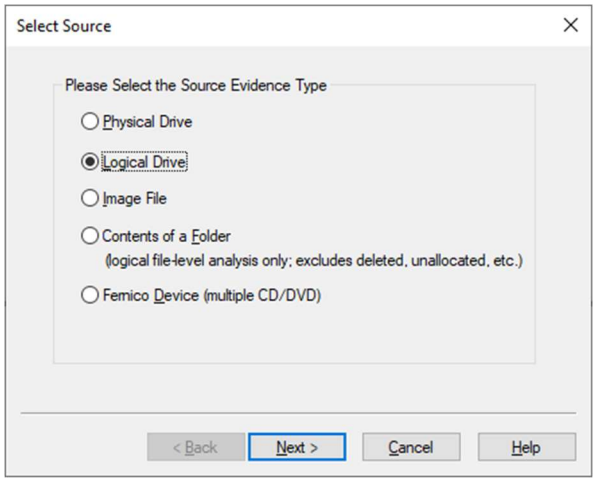
1. Open FTK Imager.



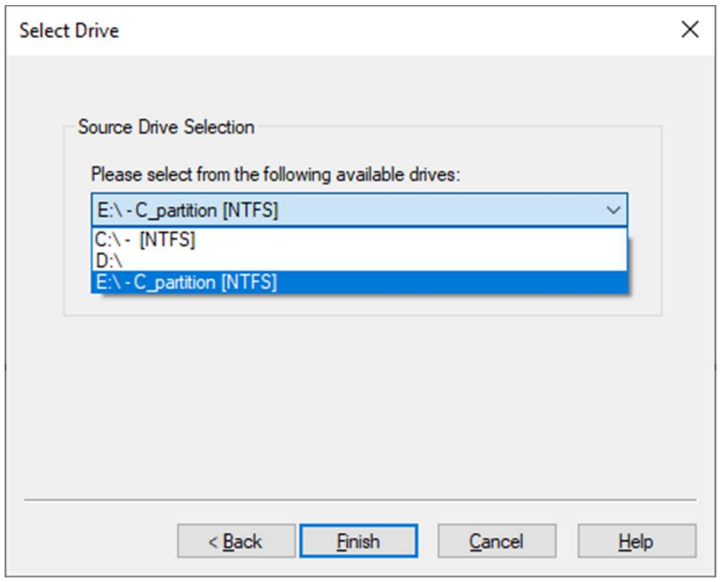
2. Select “File” -> “Create Disk Image…”



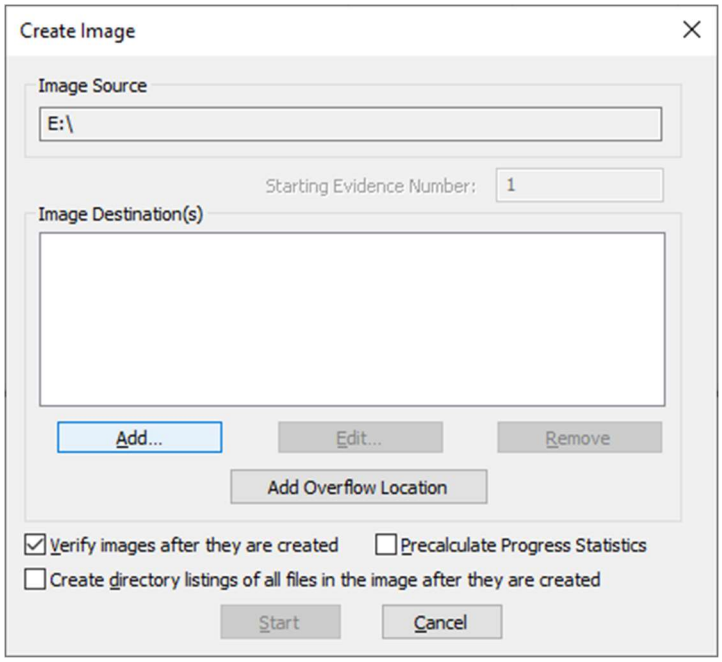
3. Select “Logical Drive”



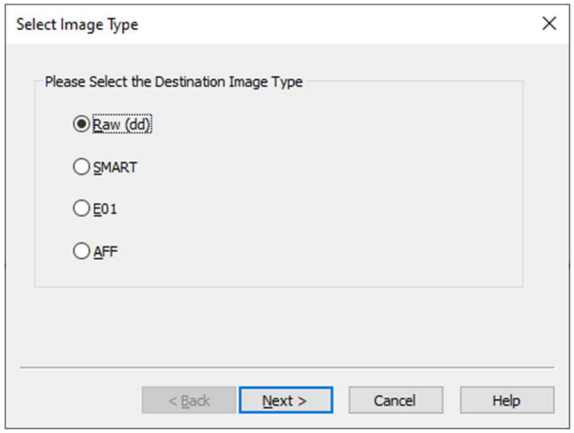
4. Select E:\ as the source drive. Click “Finish”



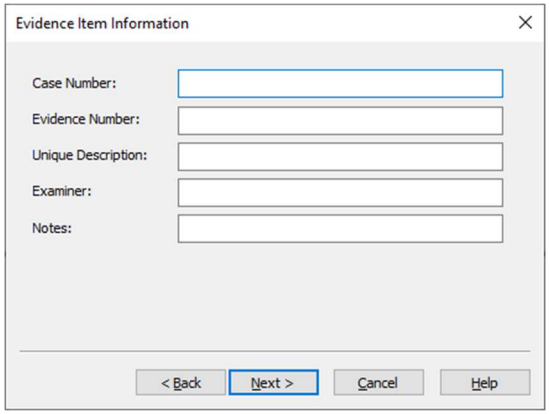
5. In the Create Image window, click on “Add” image destination.



6. Select “Raw(dd)”, click “Next”



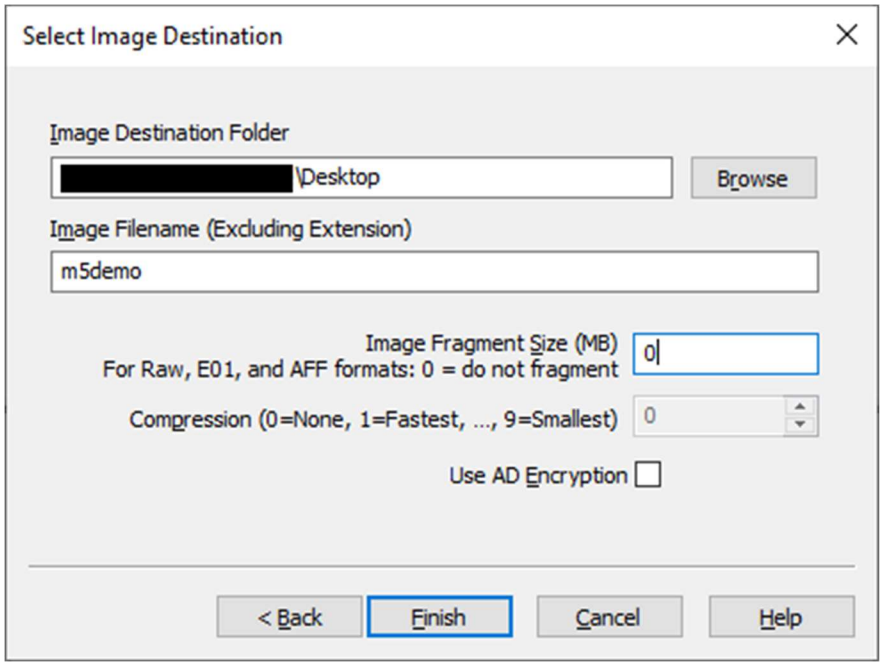
7. Leave every evidence item info blank and click “Next”



8. For the image destination folder, select under your computer desktop.

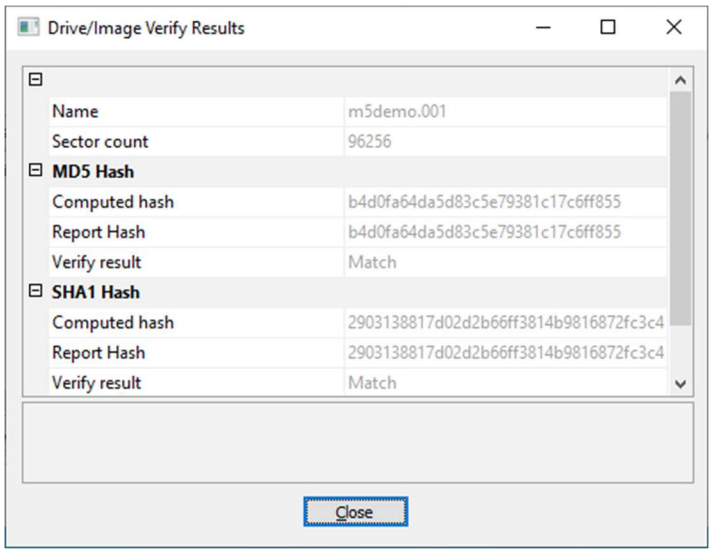
For the image filename, enter “m5demo”.

For the Image Fragment Size, enter 0. Then click “Finish”

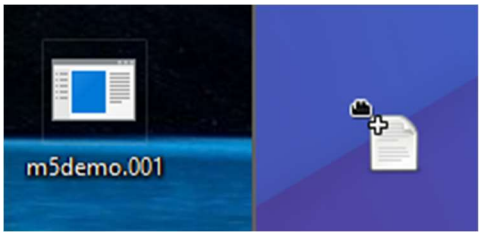


9. Then, back to the Create Image window, click “Start”

(After the process finish, you will find a m5demo.001 on the desktop)



10. Copy the m5demo.001 into your Kali Linux VM (You may drag the file into the VM directly)



Task 4. Read file signatures in the configure file of Foremost.

1. In Kali linux, open the terminal and type **sudo apt-get install foremost**

```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install foremost
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  foremost
0 upgraded, 1 newly installed, 0 to remove and 877 not upgraded.
Need to get 43.0 kB of archives.
After this operation, 103 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 foremost amd64 1.5.7-11+b1 [43.0 kB]
Fetched 43.0 kB in 1s (30.8 kB/s)
Selecting previously unselected package foremost.
(Reading database ... 302500 files and directories currently installed.)
Preparing to unpack .../foremost_1.5.7-11+b1_amd64.deb ...
Unpacking foremost (1.5.7-11+b1) ...
Setting up foremost (1.5.7-11+b1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for kali-menu (2022.3.0) ...
```

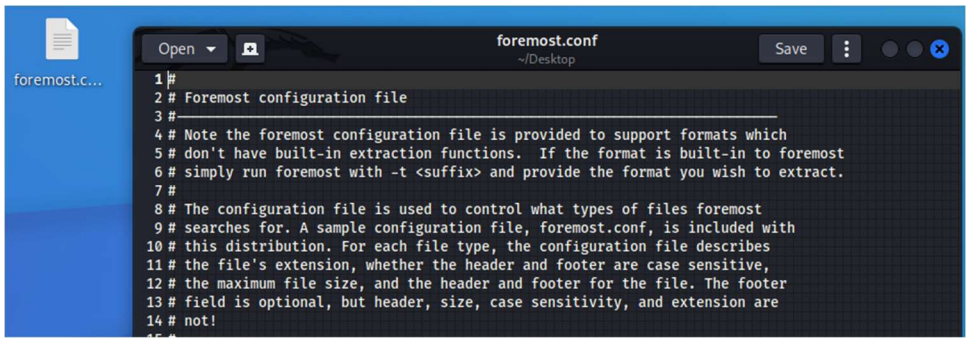
2. Enter **cd /etc/**
3. Enter **ls**

```
fonts
foremost.conf
```

4. Enter **cp foremost.conf /home/{hostname}/Desktop**

```
┌──(kali㉿kali)-[/etc]
└─$ cp formost.conf /home/kali/Desktop/
```

5. On your desktop, you should see the foremost.conf, open the document



Note: Any line that begins with a '#' is considered a comment and ignored. Thus, to skip a file type just put a '#' at the beginning of that line and if you want foremost to read specific file type, take out the '#'

6. Scroll down and find “PNG (used in web pages)” line

```
82 # PNG   (used in web pages)
83 #       (NOTE THIS FORMAT HAS A BUILTIN EXTRACTION FUNCTION)
84 #       png     y       200000  \x50\x4e\x47?   \xff\xfc\xfd\xfe
```

If you look at line 84, png represents the extension, y indicates read file case sensitive, 200000 indicates the size, \x50\x4e\x47? means the header, and \xff\xfc\xfd\xfe means the footer.

\x50\x4e\x47? is the header of png file. Those are the first few Hex digits for this file type. For more information, you can read the Magic Number Chart in the appendix. Foremost will carve files based on its header and footer.

By altering a file header or footer, software like Foremost, Scalpel will not be able to carve the files. Therefore, in that case, we need to perform manual file carving with Winhex, which will be introduced in Lab 5.5

7. Also, enable jpg and bmp files in line 78, 79, 80, 89 by take out the '#'

(You conf file should look like this)

```
74 # GIF and JPG files (very common)
75 #       (NOTE THESE FORMATS HAVE BUILTIN EXTRACTION FUNCTION)
76 #       gif     y       155000000       \x47\x49\x46\x38\x37\x61        \x00\x3b
77 #       gif     y       155000000       \x47\x49\x46\x38\x39\x61        \x00\x00\x3b
78         jpg     y       20000000        \xff\xd8\xff\xe0\x00\x10        \xff\xd9
79         jpg     y       20000000        \xff\xd8\xff\xe1 \xff\xd9
80         jpg     y       20000000        \xff\xd8        \xff\xd9
81 #
82 # PNG   (used in web pages)
83 #       (NOTE THIS FORMAT HAS A BUILTIN EXTRACTION FUNCTION)
84         png     y       200000  \x50\x4e\x47?   \xff\xfc\xfd\xfe
85 #
86 #
87 # BMP
88 #       (NOTE THIS FORMAT HAS A BUILTIN EXTRACTION FUNCTION)
89         bmp     y       100000  BM??\x00\x00\x00
90 #
```

8. Also, scroll down to line 148 to enable pdf file type. Then click “Save” on top right.

```
144 #-----------------------------------------------------------------
145 # ADOBE PDF     (NOTE THIS FORMAT HAS A BUILTIN EXTRACTION FUNCTION)
146 #-----------------------------------------------------------------
147 #
148         pdf     y       5000000 %PDF-  %EOF
149 #
150 #
```

Task 5. Carving file in image using Foremost

1. Enter **cd Desktop**

```
┌──(kali㉿kali)-[~]
└─$ cd Desktop
```

2. Enter **foremost -h** to see the help menu

```
┌──(kali㉿kali)-[~/Desktop]
└─$ foremost -h
foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus.
$ foremost [-v|-V|-h|-T|-Q|-q|-a|-w-d] [-t <type>] [-s <blocks>] [-k <size>]
        [-b <size>] [-c <file>] [-o <dir>] [-i <file]

-V  - display copyright information and exit
-t  - specify file type.  (-t jpeg,pdf ... )
-d  - turn on indirect block detection (for UNIX file-systems)
-i  - specify input file (default is stdin)
-a  - Write all headers, perform no error detection (corrupted files)
-w  - Only write the audit file, do not write any detected files to the disk
-o  - set output directory (defaults to output)
-c  - set configuration file to use (defaults to foremost.conf)
-q  - enables quick mode. Search are performed on 512 byte boundaries.
-Q  - enables quiet mode. Suppress output messages.
-v  - verbose mode. Logs all messages to screen
```

3. Enter **foremost -c foremost.conf -o foremostoutput m5demo.001**
   -c specify the configuration file to use
   -o set output directory, foreoutput in this case
   m5demo.001 is the image

```
┌──(kali㉿kali)-[~/Desktop]
└─$ foremost -c foremost.conf -o foremostoutput m5demo.001
Processing: m5demo.001
|*|
```

4. After the process is finished, you can click on the foremostoutput folder and view the file.

Questions:

1. How many **folders** are in the output folder? What are they?
2. What is the title of the pdf file?
3. What do you think if you import the image to an analysis tool like Autopsy? Does it able to show deleted files?

4. What is the difference between files carving tool like foremost and analysis tool like Autopsy?
5. Is there any way that can prevent files carved from file carving tools like foremost? (Hint: What's the difference between quick format and normal format? What does zero-out mean?)

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 2*** screenshots to document the steps.
2. In section 2, you should answer the questions above. 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.

Appendix: Magic Number Chart

Here are a few magic numbers, These are of image files.

File type	Typical extension	Hex digits xx = variable	Ascii digits . = not an ascii char
Bitmap format	.bmp	42 4d	BM
Office2007 Documents	.xlsx	50 4B 03 04 14 00 06 00	PK
GIF Format	.gif	47 49 46 38	GIF8
MP3	.mp3	49 44 33	ID3
PDF	.PDF	25 50 44 46	%PDF
JPEG File Interchange Format	.jpg	ff d8 ff e0	....
NIFF (Navy TIFF)	.nif	49 49 4e 31	IIN1
PM format	.pm	56 49 45 57	VIEW
PNG format	.png	89 50 4e 47	.PNG
Postscript format	.[e]ps	25 21	%!
Sun Rasterfile	.ras	59 a6 6a 95	Y.j.
Targa format	.tga	xx xx xx	...
TIFF format (Motorola - big endian)	.tif	4d 4d 00 2a	MM.*
TIFF format (Intel - little endian)	.tif	49 49 2a 00	II*.
X11 Bitmap format	.xbm	xx xx	
XCF Gimp file structure	.xcf	67 69 6d 70 20 78 63 66 20 76	gimp xcf
Xfig format	.fig	23 46 49 47	#FIG