

## **Lab 5-Module 5.4: QPhotoRec**

### **Objectives**

- File carving using PhotoRec

### **Task**

#### **Task 1. Software Preparation**

Image included:

- Lake.png
- Fun.bmp
- testpdf.pdf
- text.txt

You may choose CAINE or Windows to perform this lab.

#### **CAINE:**

CAINE has pre-installed PhotoRec. No additional download needed.




#### **Windows:**

1. Download PhotoRec from the official website:  
[https://www.cgsecurity.org/wiki/TestDisk\\_Download](https://www.cgsecurity.org/wiki/TestDisk_Download), then unzip the folder to desktop
2. Download the image and put it on desktop
3. Create a folder on desktop called “photoRecOutput” to store the recover files

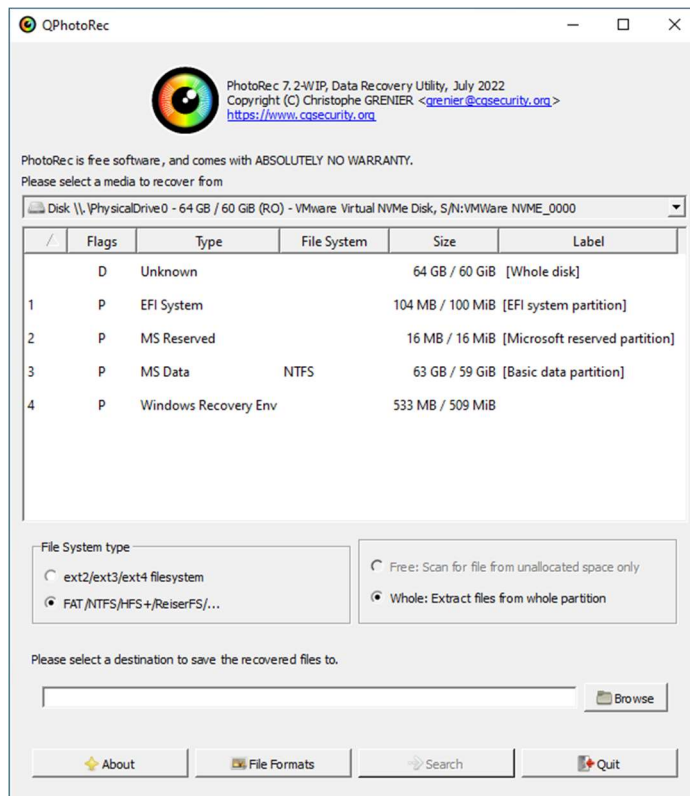


4. Open testdisk folder and open **qphotorec\_win.exe**

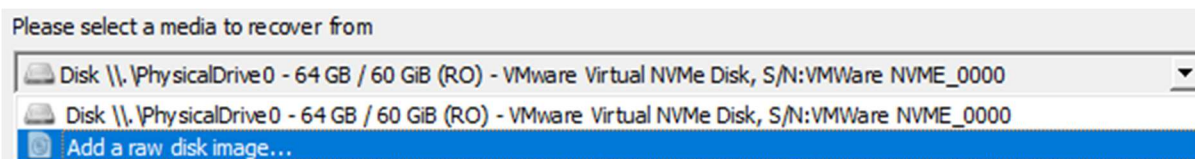
(Note: photorec\_win.exe is the command line application and qphotorec is the GUI application)

 photorec_win.exe	Application	1,114 KB
 qphotorec_win.exe	Application	995 KB
	CONF FILE	1 KB

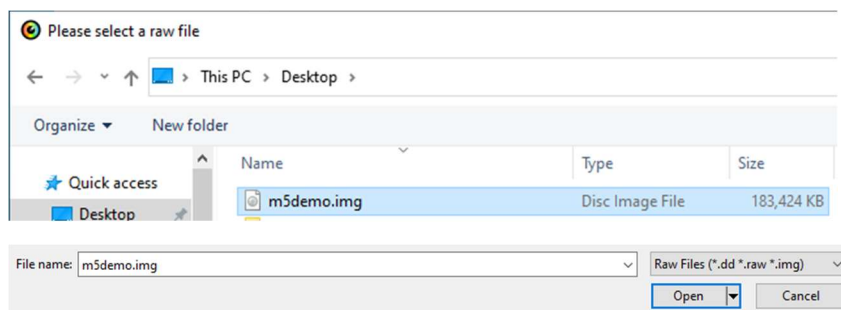
## Task 2: File carving using PhotoRec



1. Click select a media to recover from and select **“Add a raw disk image...”**



2. Select the image we prepared in step 2 and then click “Open”



3. Select the item that has Flags P(which stand for petition) and the File System is NTFS

/	Flags	Type	File System	Size	Label
D		Unknown		187 MB / 179 MiB	[Whole disk]
P		NTFS	NTFS	187 MB / 179 MiB	

4. Select **FAT/NTFS/HFS+/ReiserFS/...** and select **Free: Scan for file from unallocated space only**

File System type	
<input type="radio"/> ext2/ext3/ext4 filesystem	<input checked="" type="radio"/> Free: Scan for file from unallocated space only
<input checked="" type="radio"/> FAT/NTFS/HFS+/ReiserFS/...	<input type="radio"/> Whole: Extract files from whole partition

5. For the destination, click **browse** and select the folder we created in step 3.

Please select a destination to save the recovered files to.

**photoRecOutput** File folder

Folder:

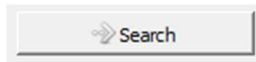
6. Click on File Formats and you can check all the file formats which photoRec supports.

☒ File Formats

QPhotoRec: File Formats

<input checked="" type="checkbox"/> custom Own custom signatures
<input checked="" type="checkbox"/> 1cd Russian Finance 1C:Enterprise 8
<input checked="" type="checkbox"/> 3dm Rhino / openNURBS
<input checked="" type="checkbox"/> 3ds 3d Studio
<input checked="" type="checkbox"/> 7z 7zip archive file
<input checked="" type="checkbox"/> DB
<input checked="" type="checkbox"/> a Unix Archive/Debian package
<input checked="" type="checkbox"/> abr Adobe Brush
<input checked="" type="checkbox"/> acb Adobe Color Book
<input checked="" type="checkbox"/> accdb Access Data Base
<input checked="" type="checkbox"/> ace ACE archive
<input checked="" type="checkbox"/> ...

7. Keep the default setting and click OK, then click Search to start the data recovery process. The process may take some time but should not be longer than 3 mins



8. After it is finished, it will list the file type that has successfully recovered and the number of files. Click “Quit” to exit the application.



9. Open “**photoRecOutput**” folder on desktop and

Question:

1. How many files does photoRec successfully recover?
2. Which file format does photoRec **cannot** be recovered?