

PhotoRec – Deleted Data Recovery Tool Guide

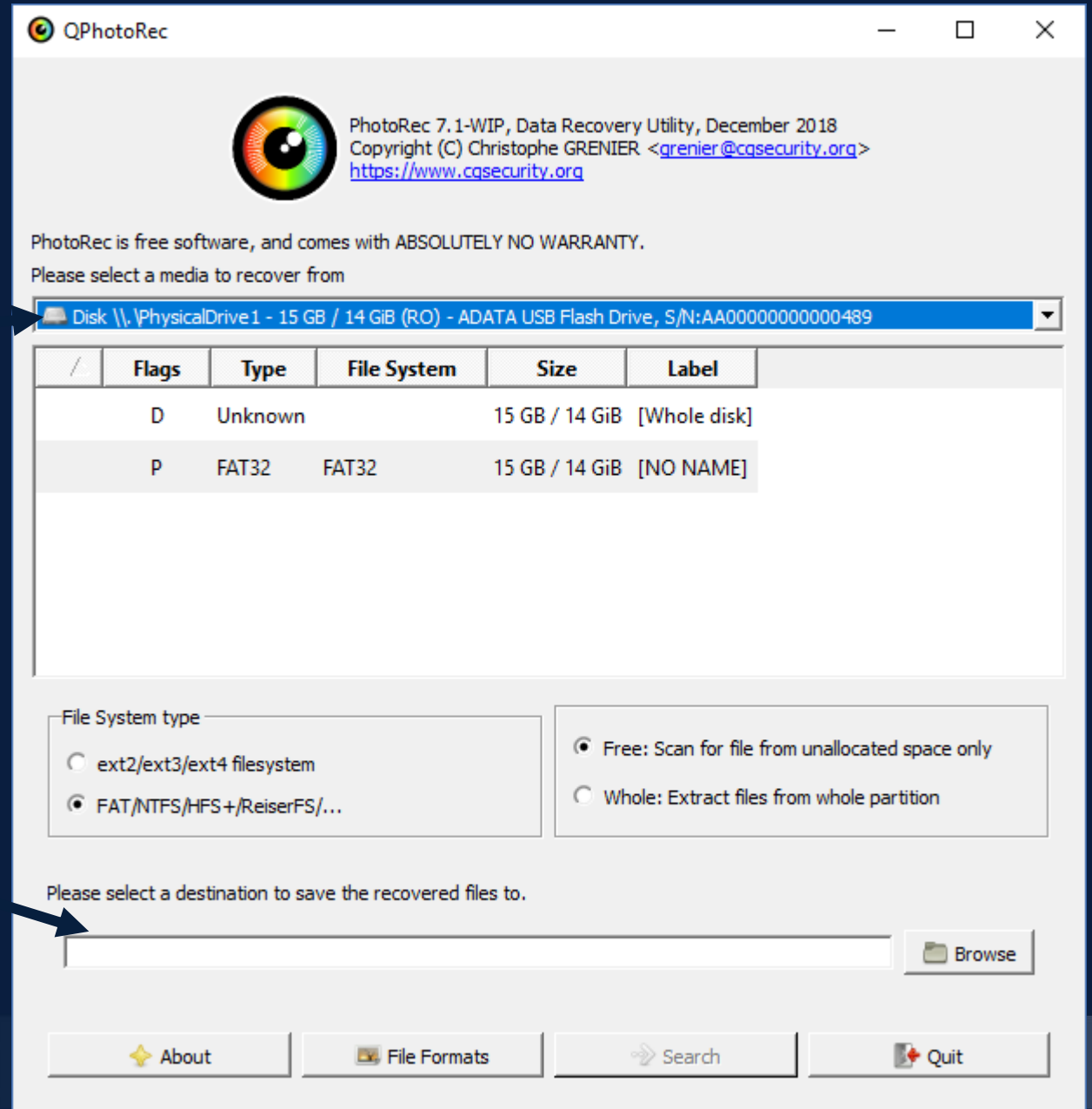
Installing PhotoRec?

- Unzip the “testdisk-7.1-WIP.win.zip” file
- PhotoRec comes bundled with the TestDisk program (which we will not be using)
- It is not “installed” so it could technically be a portable utility run from a thumb drive
- PhotoRec can run in the command line, but it also has a GUI – qphotorec-win.exe

platforms	2/2/2019 10:49 AM	File folder
plugins	5/19/2008 2:38 AM	File folder
.travis.yml	4/5/2017 8:26 AM	YML File
AUTHORS.txt	2/2/2019 10:49 AM	Text Document
COPYING.txt	2/2/2019 10:49 AM	Text Document
cygwf-2.dll	11/25/2016 1:20 AM	Application extens...
cyggcc_s-1.dll	12/4/2017 7:01 PM	Application extens...
cygiconv-2.dll	12/5/2017 1:18 AM	Application extens...
cygjjpeg-8.dll	11/25/2016 1:19 AM	Application extens...
cygncursesw-10.dll	12/5/2017 2:03 AM	Application extens...
cygssp-0.dll	12/4/2017 7:01 PM	Application extens...
cygwin1.dll	12/5/2017 12:01 AM	Application extens...
cygz.dll	12/5/2017 1:12 AM	Application extens...
documentation.html	12/24/2017 9:21 AM	Chrome HTML Do...
fidentify_win.exe	2/2/2019 10:49 AM	Application
iconv.dll	7/14/2018 11:01 AM	Application extens...
INFO	2/28/2018 2:30 AM	File
libbz2-1.dll	7/14/2018 10:27 AM	Application extens...
libewf-2.dll	6/29/2018 7:59 AM	Application extens...
libfonttype-6.dll	11/1/2018 4:04 PM	Application extens...
libgcc_s_sjlj-1.dll	9/5/2018 8:08 AM	Application extens...
libglib-2.0-0.dll	1/22/2019 7:44 AM	Application extens...
libharfbuzz-0.dll	8/9/2018 10:18 AM	Application extens...
libintl-8.dll	7/14/2018 10:45 AM	Application extens...
libjpeg-62.dll	1/11/2019 6:42 AM	Application extens...
libpcre-1.dll	7/14/2018 10:49 AM	Application extens...
libpcre2-16-0.dll	7/14/2018 10:54 AM	Application extens...
libpng16-16.dll	7/14/2018 10:44 AM	Application extens...
libssp-0.dll	9/5/2018 8:08 AM	Application extens...
libstdc++-6.dll	9/5/2018 8:08 AM	Application extens...
libwinpthread-1.dll	7/14/2018 10:58 AM	Application extens...
NEWS.txt	2/2/2019 10:49 AM	Text Document
photorec-win.exe	2/2/2019 10:49 AM	Application
qphotorec-win.exe	2/2/2019 10:49 AM	Application

Run PhotoRec

- From the drop down, select your drive (mounted forensic image with FTK Imager)
- You can pretty much leave all the other defaults
- Select a location to write the files to (I recommend a folder on the desktop)



About PhotoRec

- PhotoRec is a free open-source tool available for a variety of operating systems
 - Including version for MacOS and Linux
- Automatically does a “deep scan” ignoring the file system and carving all possible data
- Has the ability to import custom file headers to search for different file types
- Scans are thorough – can take a long time
- Built into some forensic tools for carving

Acknowledge:

- Matt Ruddell
- Questions? mr Ruddell@fiu.e