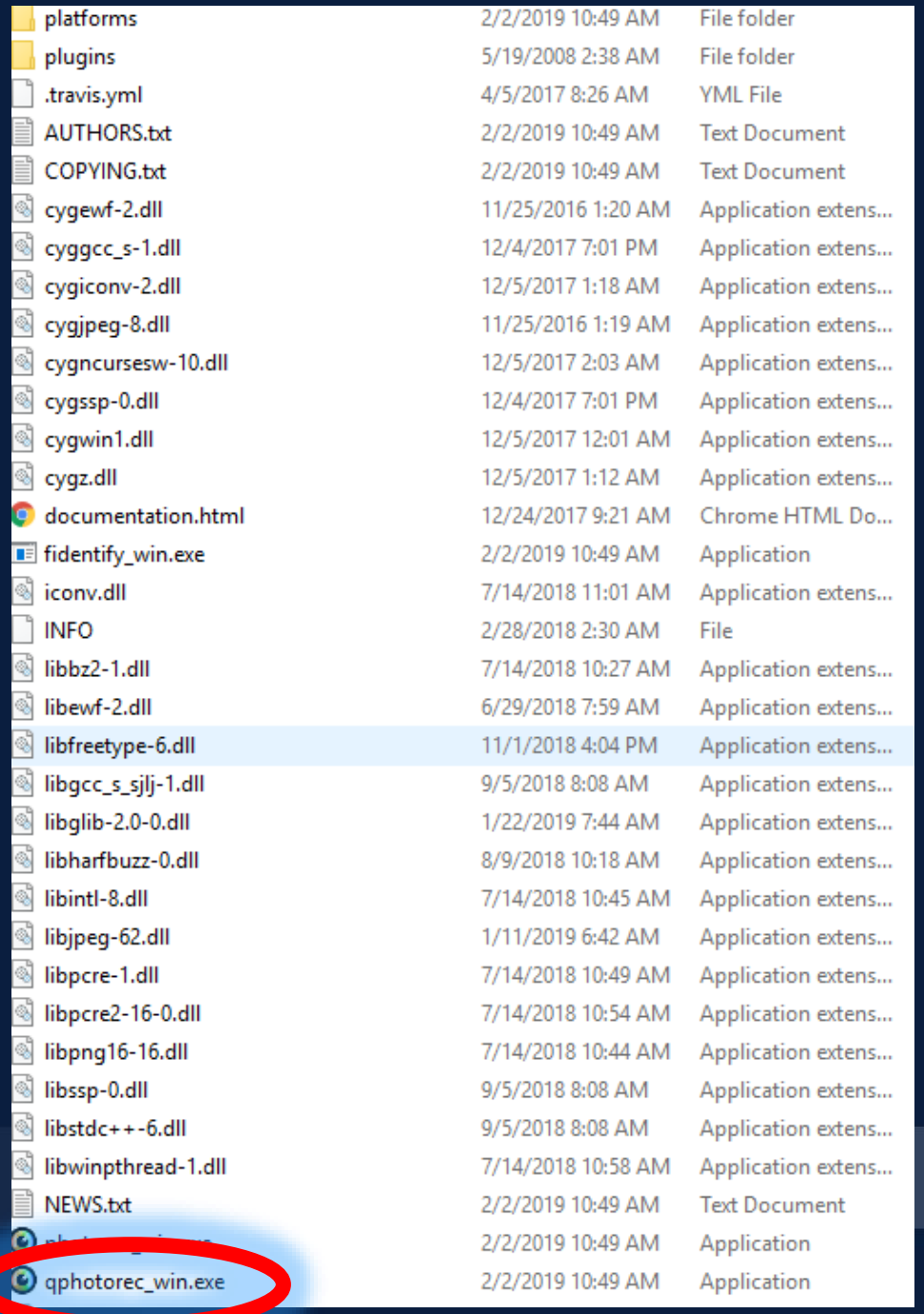
PhotoRec – Deleted Data Recovery Tool Guide

Installing PhotoRec?

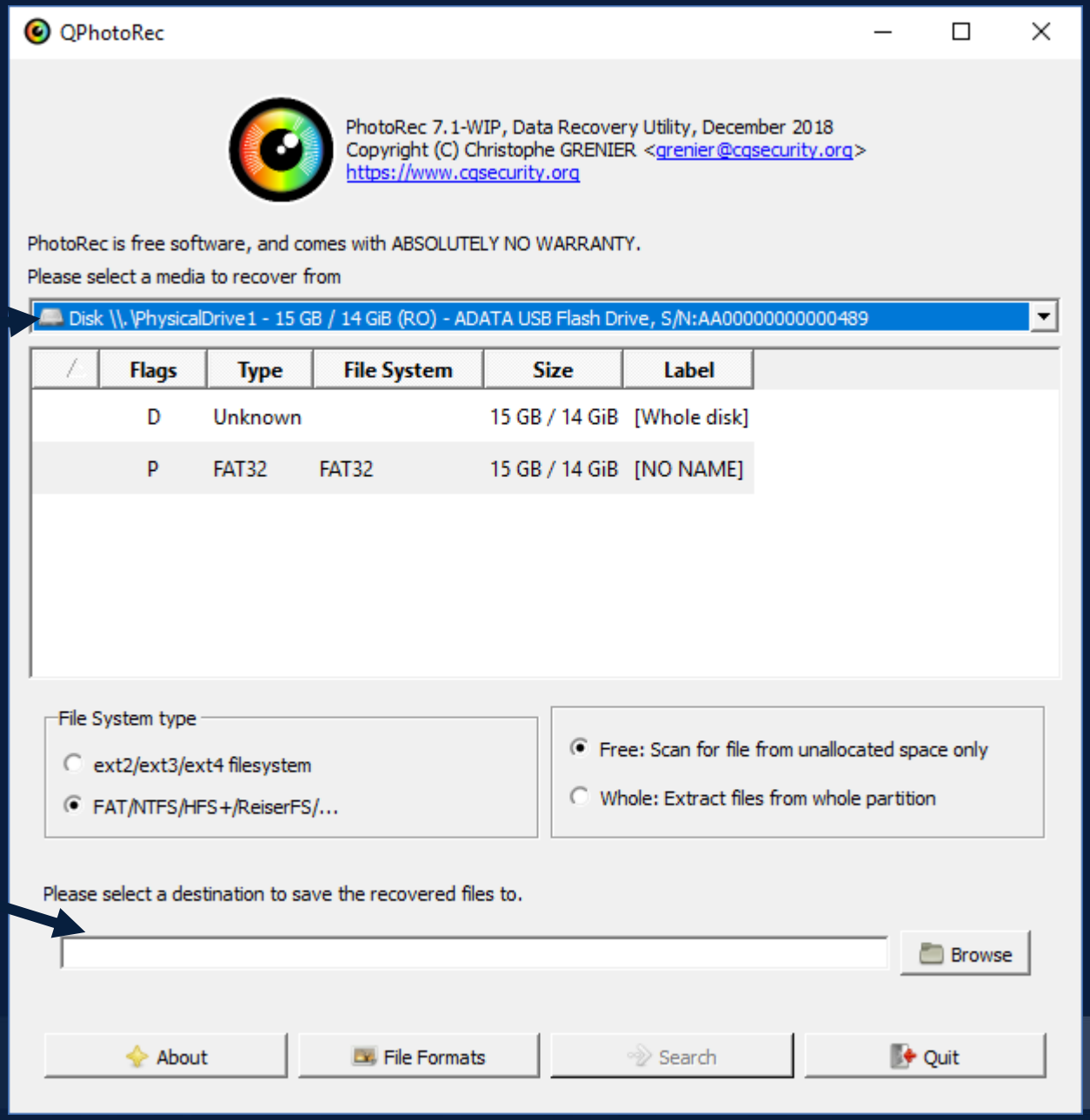
- Unzip the “testdisk-7.1-WIP.win.zip” file
- PhotoRec comes bundled with the TestDisk program (which we will not be using)
- It is not “installed” so it could technically be a portable utility run from a thumb drive

- PhotoRec can run in the command line, but it also has a GUI – qphotorec-win.exe



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
- mruddell@fiu.e

Questions??