MICT1 Group 3

EXERCISES WEEK 4

Chris Kuipers
Juul Steins
Mick Ubags

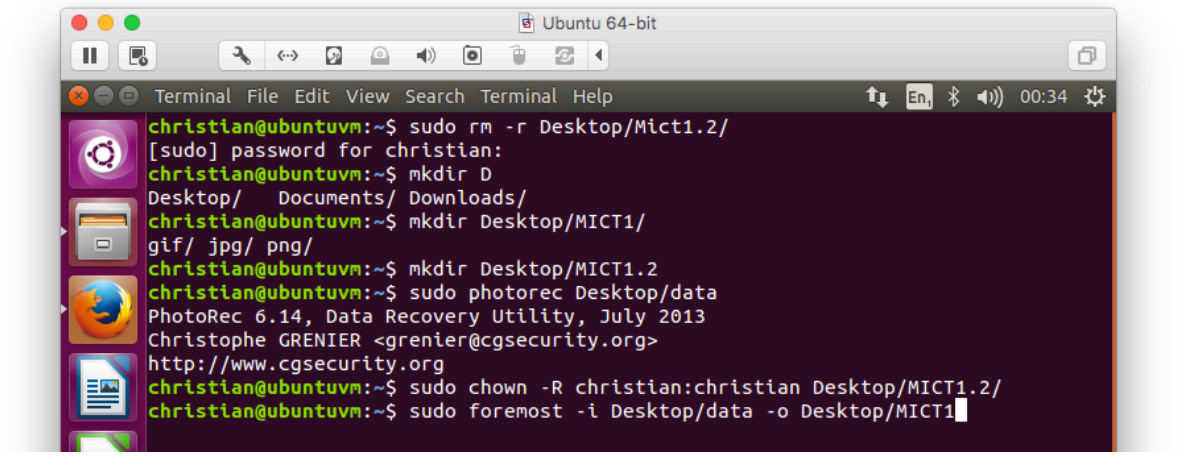
Assignment

Investigate the provided file “data”, which contains a dump of 162 clusters of 4k from an unknown file system.

See if you can find some usable files that could have been in either RAM- and/or Disk-slack. Report your findings.

Method

We analyzed the supplied file with *Synalyze It!*. Synalyze It! is a hex editor for Mac OS X. Using UTF-8 encoding we scrolled through the binary file until we discovered JFIF text strings, which seemed to indicate we were looking at possibly multiple JPEG files. Using the JFIF file format we tried to extract the images without success. After some trail and error we chose for a different approach: We fired up our good old Ubuntu virtual machine and used a File Carver to carve the image for usable files. The carver of our choice was foremost.
https://en.wikipedia.org/wiki/JPEG_File_Interchange_Format
https://www.w3.org/Graphics/JPEG/jfif3.pdf



Results

Obviously we recoverd the starwars jpeg files. We got two jpeg files which are, apart from their size, pretty much equal to eachother. It looks like the latter jpeg is the thumbnail image of the first:

While investigating the metadata of the image using our hex editor we discovered the jpeg files have been edited, or at least been opened with Adobe Creative Cloud Photoshop.

The evidence file also contained a png image file. There is not much to this image since the resolution is only 1 by 1 pixel. Lastly the image contained a corrupted GIF file which we were unable to restore or recover any useful information.