Instruction

1. Run this,
   $ su root (password is amrita123)
   $ apt-get install binwalk exiftool ghex steghide
   $ Press Ctrl+D or type exit
2. For tutorial 1 and 2 download any image from internet.
3. Document all your work (including tutorial) in a word file and send it to shankaraman.r@gmail.com

Questions

1. Identify the type of files using file (try with any files you want and understand the output)

   $ file your_file_goes_here

2. The header for the file is damaged. Fix it and submit the message.
   a. Read about file signatures (Check references section [2])
   b. Use hexedit
3. Download the pcap file (or see references section [1] to download the file)
   a. What are the IP address , MAC address, Port no's of the communicating parties?
   b. What are the protocols present in the pcap file?
   c. Can you find the username and password from the pcap file?
4. List the partion details about your machine.
   $ fdisk -l or $ df -h
5. Give the latitude and longitude from the image file. (Check reference section [3])

Tutorial 1:

$ cat the_image_file.png your_zip_file.zip > new_file.png

Extracting:

$ binwalk your_image_file.png

$ dd if=your_image_file.png of=secret.zip bs=1 skip=(offset you got after running binwalk)

Tutorial 2:

$ steghide embed -cf your_image.jpg -ef secret.txt

Enter a password when it prompts and remember it.

Enter a password:

Extracting:

Enter the password you supplied later

$ steghide extract -sf your_image.jpg

Enter a password:

References

[1] https://github.com/shankaraman/Downloads/blob/master/intercept.pcap
[2] http://en.wikipedia.org/wiki/List_of_file_signatures
[3]https://github.com/shankaraman/Downloads/blob/master/2014-02-12_09-18-48_534.jpg