COMP 597 - Computer Forensics
Assignment #2

Spring 2017

Due Date: Thursday, February 23, 2017

Total Points: 100

Question 1

Answer the following question based on *q1.dd* image that contains a modified extended partition table:

1. How many sectors are there in this image?
2. Use *fdisk*, *mmls*, *FTK Imager*, *DFF* and *Encase Imager* to determine how many partitions are there. Document all the results from the different tools then analyze and compare the tools' results.
3. Go through the partition table\s manually by hand and construct the partition table. Two of the table entries are incorrect on purpose. Fixing the two mistakes might uncover more partitions. Try to find the mistakes, fix them, then display the contents of the partitions showing the following information for each partition:

Boot	Start	End	Size	Type

4. Fix the image by correcting the mistakes from part 3; this can be done by using a Hex editor. Then, use *fdisk*, *mmls*, *FTK Imager*, *DFF* and *Encase Imager* to determine how many partitions are there. Document all the results from the different tools then analyze and compare the tools' results.

Question 2

Given *q2.dd*:

1. How many sectors are there in this image?
2. Calculate the partition table by hand and display its contents showing the all the partitions and any unallocated/slack space. Document your result using the following table:

Start	End	Size	Type

3. There are some hidden information on this image. Locate this information, indicate their type, and where they are located. Make sure to document in details the steps you took to uncover the data.

What to hand in

Submit your project electronically through Canvas. Please hand in the following:

- A report for each question.
- In addition to the contents of the reports, their grade will also be based on their readability and formatting/presentation.