**Lab 6: Recognizing the Use of Steganography in Image Files**

**By**

**Natnael Kebede**



**University of Dallas**

**2020**

This Paper Submitted in Partial Fulfillment of the Requirements for

CYBS 7359 – Penetration Testing and Vulnerability Assessment

Spring 2020

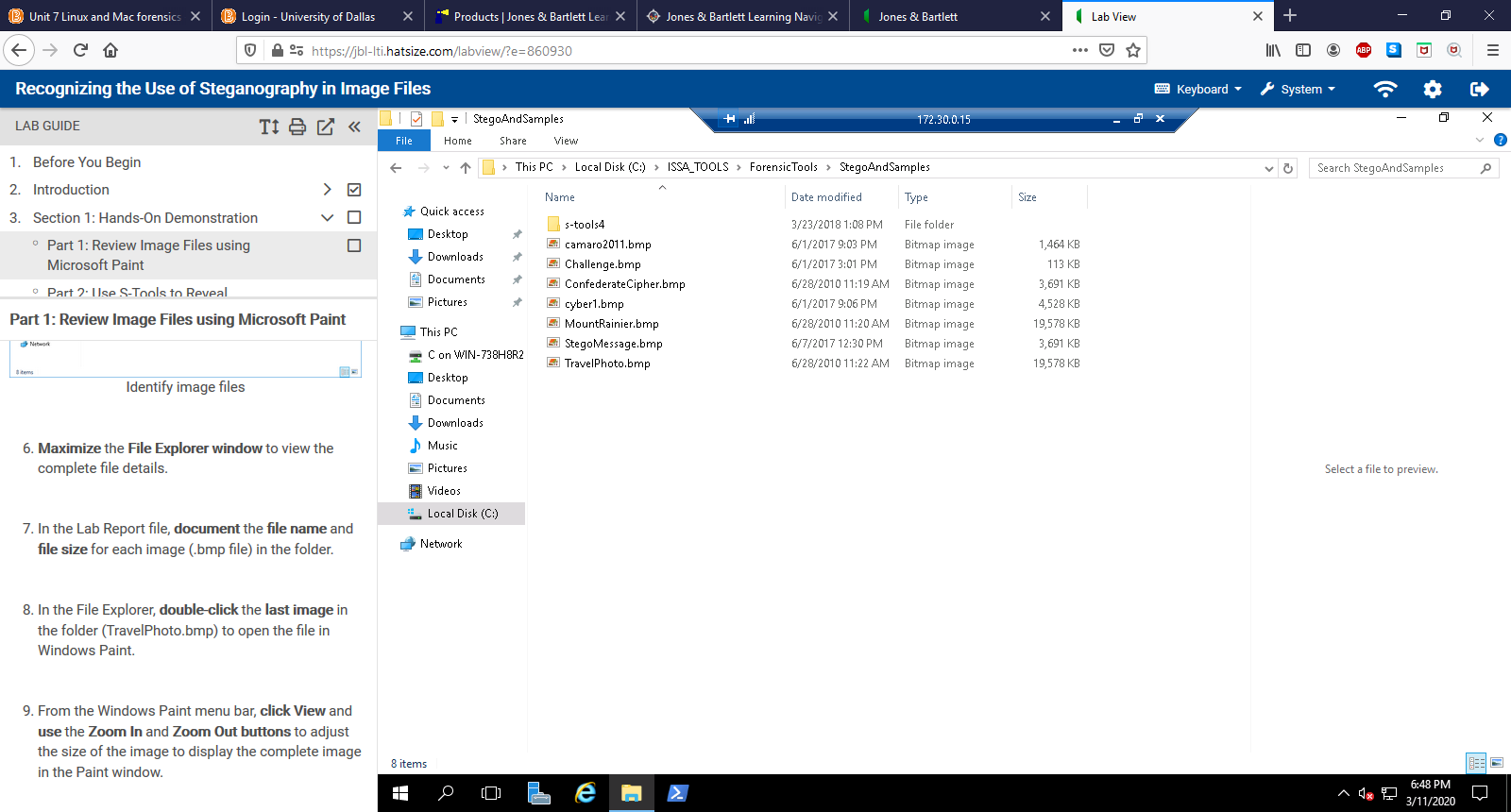
Presented to Dr. Renita Murimi

**Section 1**

**Part 1**

1. In the Lab Report file, document the file name and file size for each image (.bmp file) in the folder.

Each Bitmap image file name and its associated size is shown in the screenshot below.



1. In the Lab Report file, describe the content of the image.

All the contents of the image files are detailed below.

The **TravelPhoto.bmp** image is a photo of a town being overlooked by a mountain with snow ice caps.

The **camaro2011.bmp** image is a photo of a silver Chevrolet Camaro with a plate of USA1.

The **Challenge.bmp** image is a photo of a red old school challenger with white stripes in the center.

The **ConfederateCipher.bmp** image is a photo of a large disk with 2 sets of the alphabet and is a confederate cipher disk used for cryptography.

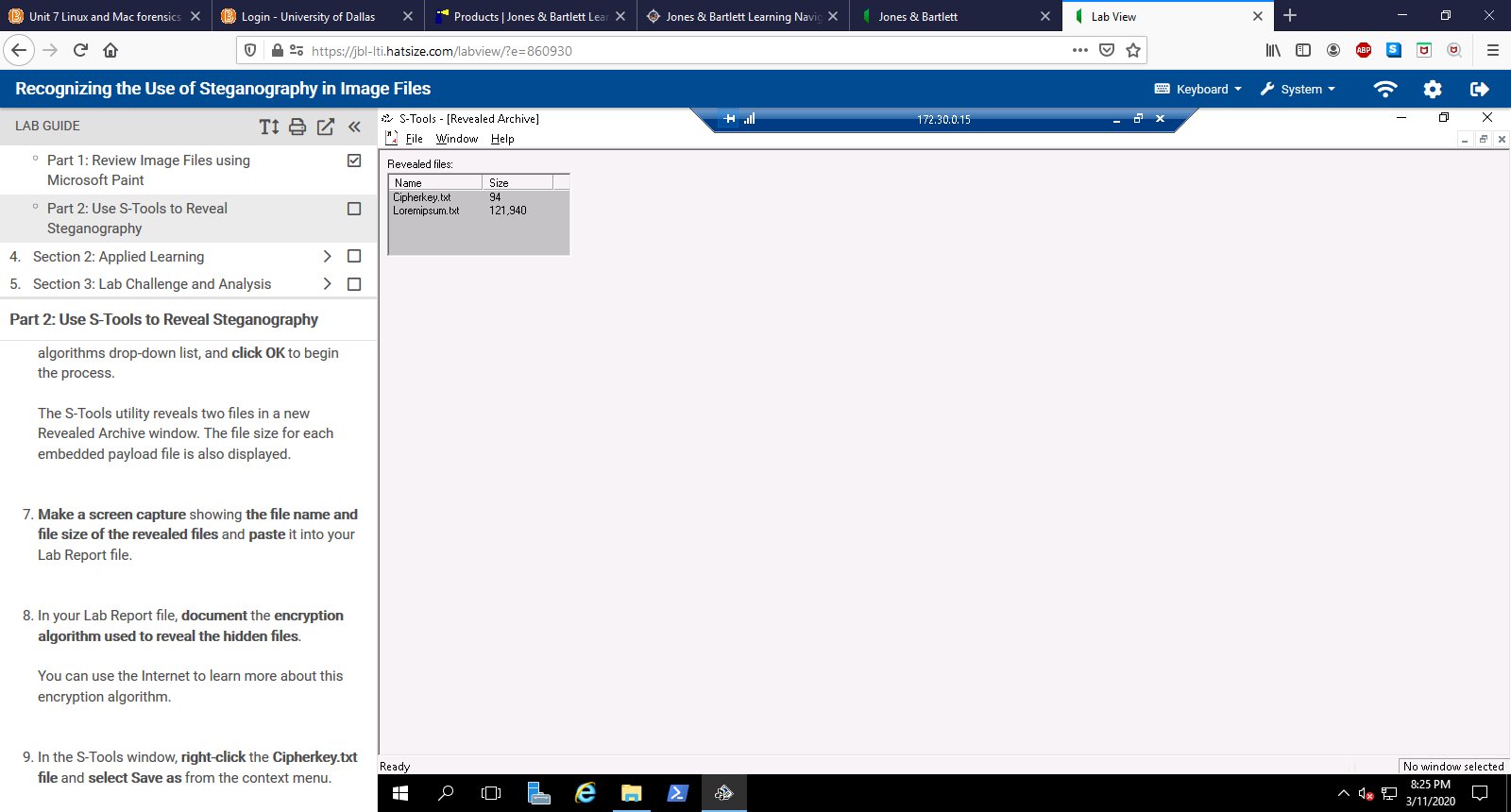
The **cyber1.bmp** image is a photo of a person in a hoodie in the dark with an Ultrabook against a large screen with 0s and 1s displaying on both the screen and the Ultrabook.

The **MountRainier.bmp** image is a photo of a town being overlooked by a mountain with snow ice caps. This content of this image is the same as the one displayed in **TravelPhoto.bmp**

The **StegoMessage.bmp** image is a photo of a large disk with 2 sets of the alphabet and is a confederate cipher disk used for cryptography. This content of this image is the same as the one displayed in **ConfederateCipher.bmp**

**Part 2**

1. Make a screen capture showing the file name and file size of the revealed files and paste it into your Lab Report file.



1. In your Lab Report file, document the encryption algorithm used to reveal the hidden file.

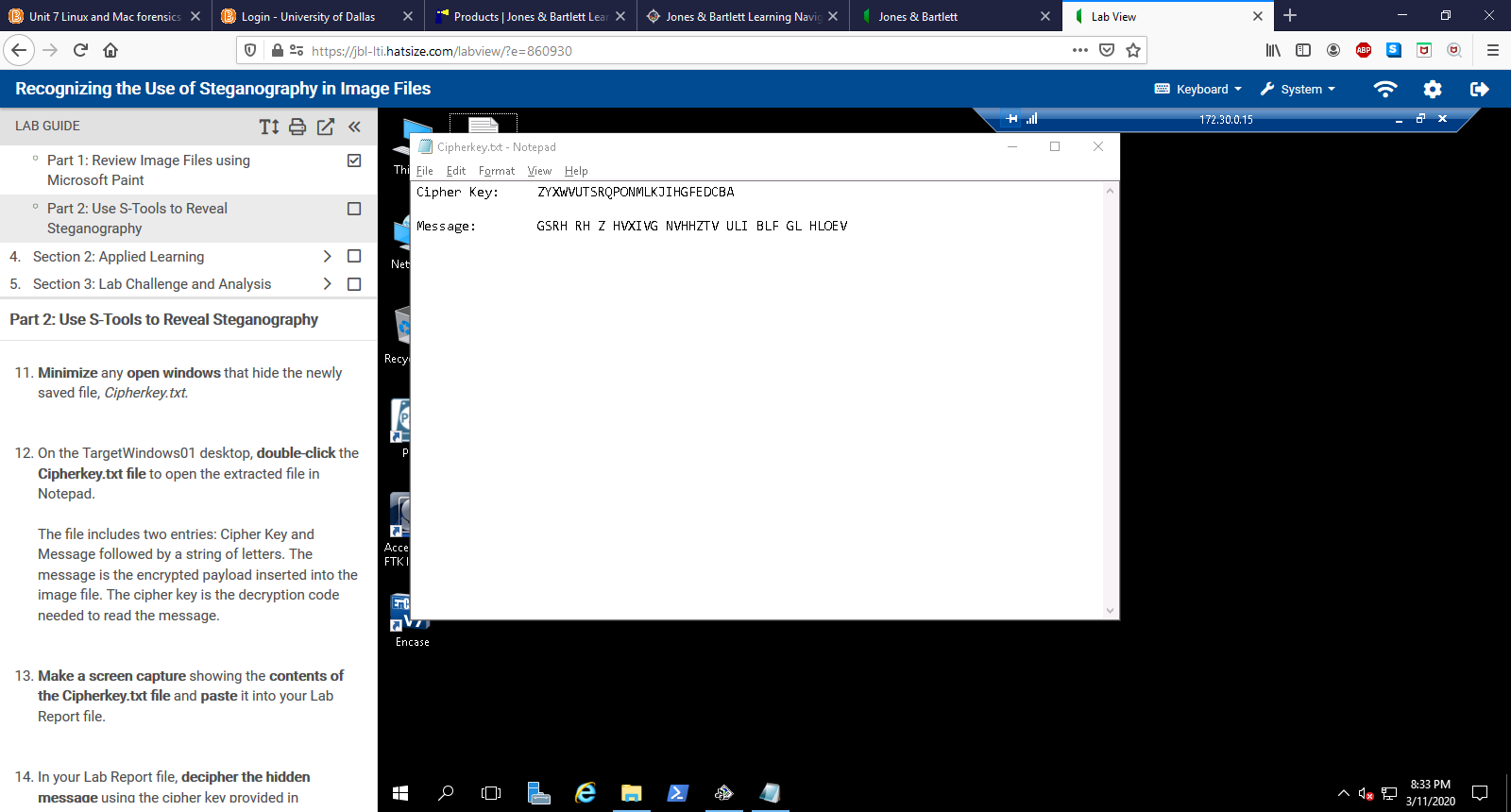
The IDEA (International Data Encryption Algorithm) is a symmetric encryption algorithm developed at ETH in Zurich, Switzerland. It uses a block cipher (64-bit blocks of data divided into smaller blocks) with a 128-bit key-space and is generally considered to be very secure (Aumasson, 2018). It is considered among the best publicly known algorithms. In the several years that it has been in use, no practical attacks on it have been published despite of the number of attempts to find some. IDEA is patented in the United States and in most of the European countries (Rouse & Pronk, 2005).

References

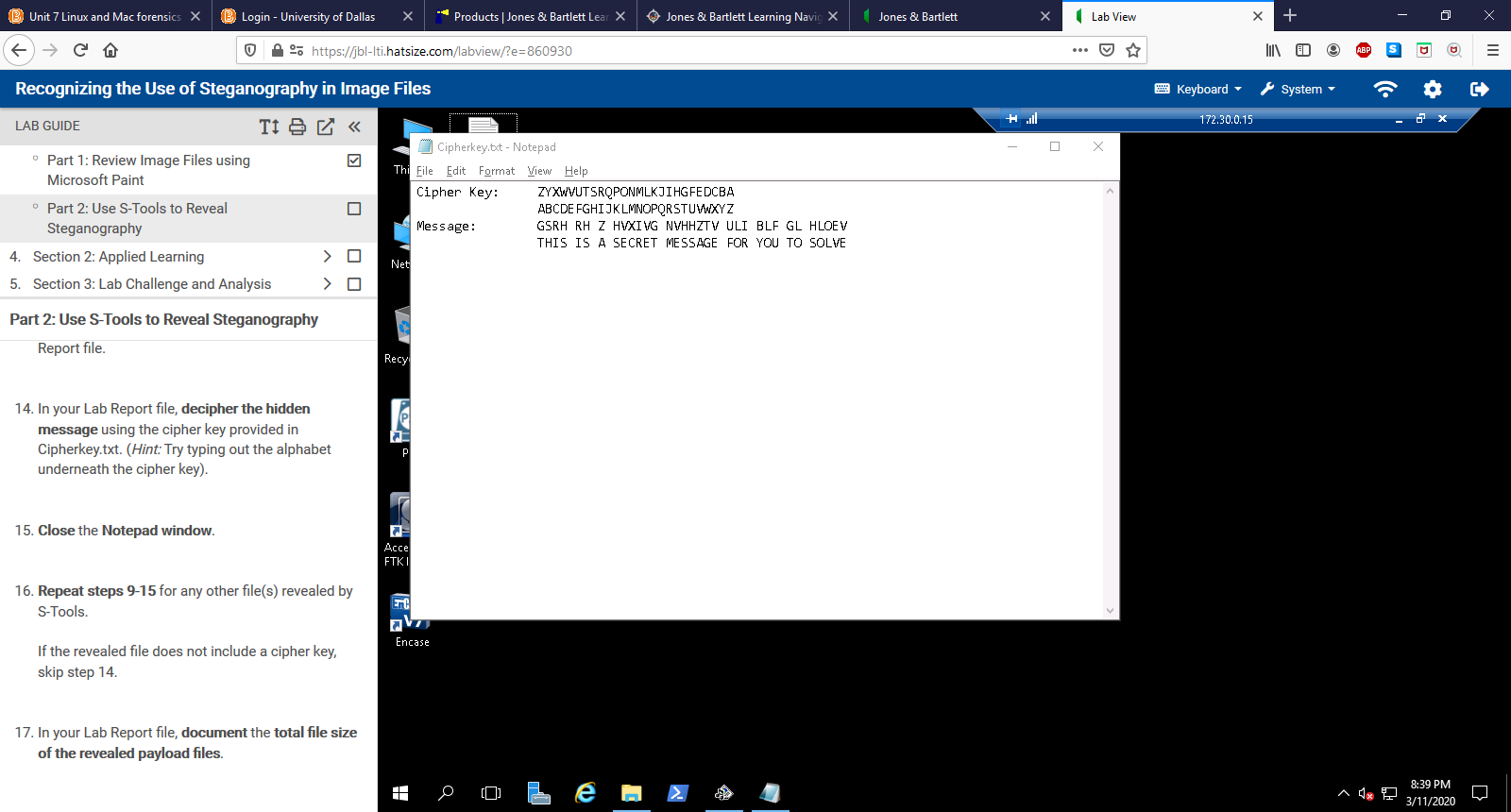
Aumasson, Jean-Philippe. (2018). *Serious Cryptography*. San Francisco, CA: No starch press.

Rouse, M., & Pronk, O. (2005). What is International Data Encryption Algorithm (IDEA)? - Definition from TechTarget. Retrieved from <https://searchsecurity.techtarget.com/definition/International-Data-Encryption-Algorithm>

1. Make a screen capture showing the contents of the Cipherkey.txt file and paste it into your Lab Report file.



1. In your Lab Report file, decipher the hidden message using the cipher key provided in Cipherkey.txt. (*Hint:* Try typing out the alphabet underneath the cipher key).

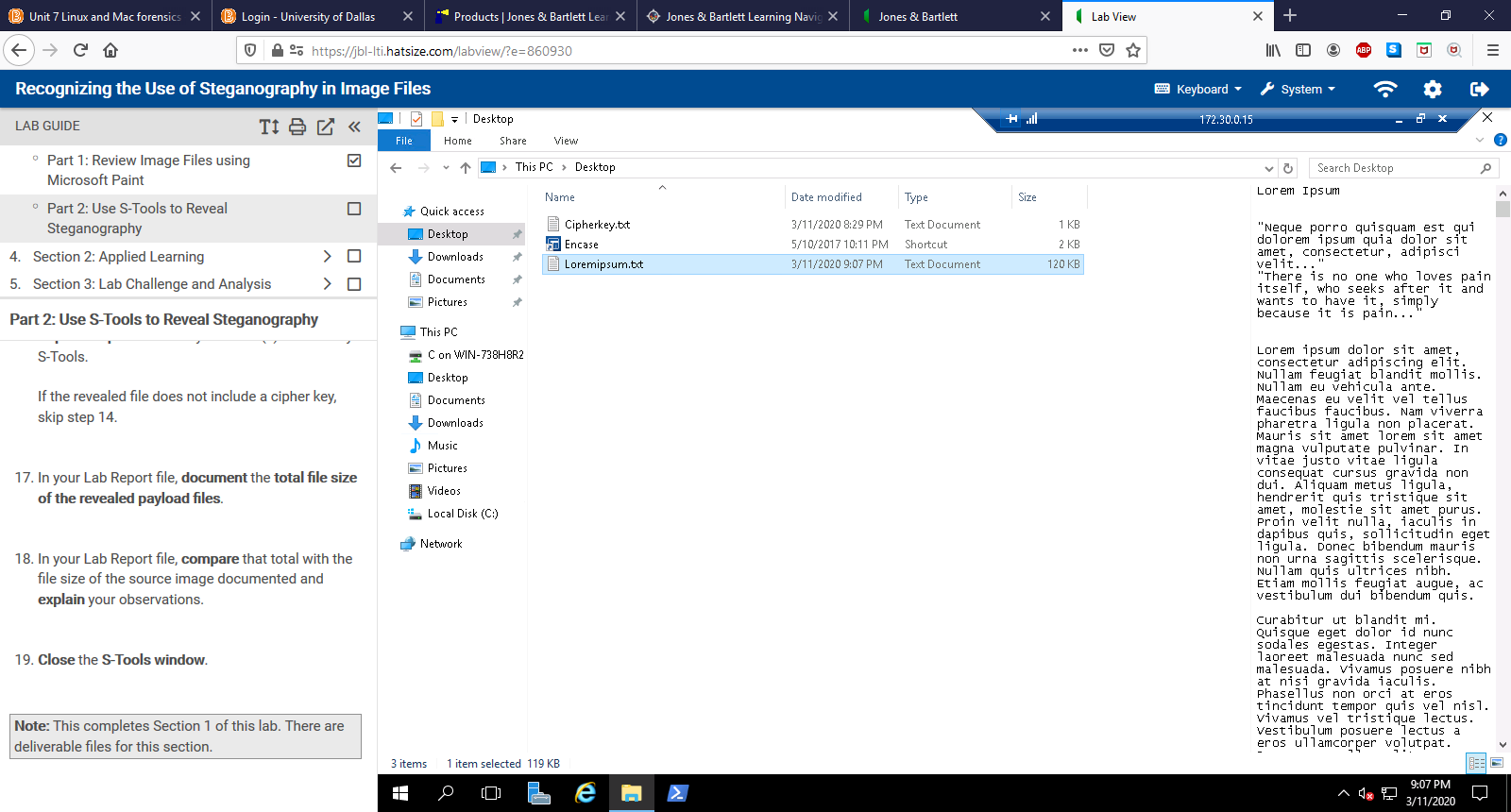


1. In your Lab Report file, document the total file size of the revealed payload files.

The total size of the revealed payload files from StegoMessage.bmp image (the only file that has steganography) is shown below.

Cipherkey.txt: 1KB

Loremipsum.txt: 120 KB



1. In your Lab Report file, compare that total with the file size of the source image documented and explain your observations.

Comparing the payload file sizes above with the original source image (StegoMessage.bmp) we can see that the total file size of StegoMessage.bmp is 3,691 KB, while the payload files are a very small amount of that: 1KB and 120 KB respectively. This is due to the nature of the payload files being plain text (.txt) files with only text in them. Hence, one can conclude that the payload files size is very small when compared to the original source image.