

## **ABSTRACT**

*Data received from various sources such as Google is not necessarily completely protected from viruses. Even though antivirus has been circulating a lot, it is not certain to find out if there are hidden messages behind the files that we download from search engines. Steganography is the art and science of writing hidden messages so that only the sender and recipient are aware of the presence or absence of hidden messages in files that we download from search engines. To anticipate this, it can be done by using the steganalysis method. Steganalysis is one solution that can be used to monitor and identify messages that are suspected of carrying hidden messages behind the file.*

*In this thesis research, an analysis of statistical values possessed in an audio file that has the .wav format detected by the message and the position of the message is located. From the value obtained, the value is used to view audio files that have the original .wav format and which have been inserted messages (stegoed files) with the LSB insertion process. In this research, a software that is able to detect the presence of hidden messages and the position of the preparation is made using the MFCC method with the Decision Tree classification.*

*In this Final Project research designed a system that is able to identify secret messages in audio files with .wav format using MFCC and Decision Tree methods. The system created produces the best performance with an accuracy level of 76.52% for steganalysis. For position detection, the best accuracy is 94.73% from the test data identified as stego-audio. As for the detection of the position position, the accuracy is 56.58%.*

***Keyword: Steganography, Steganalysis, Mel-Frequency Cepstral Coefficient, Decision Tree.***