Steganography and Watermarking

Extracting all the files:

Graphical user interface

Description automatically generated

^Using ftp-data parameters to search for any potential files that are being sent across.

A screenshot of a computer

Description automatically generated

^Using tcp Follow in order to download the file as raw.

Graphical user interface, application, website

Description automatically generated

^Saving intercepted file as raw

Graphical user interface, application, Teams

Description automatically generated

^Obtained a zip and extracted

A picture containing text, sign

Description automatically generated

Graphical user interface, text, application

Description automatically generated

^Received a .msg file and saved using outlook to obtain the .bmp file.

Text

Description automatically generated

Text

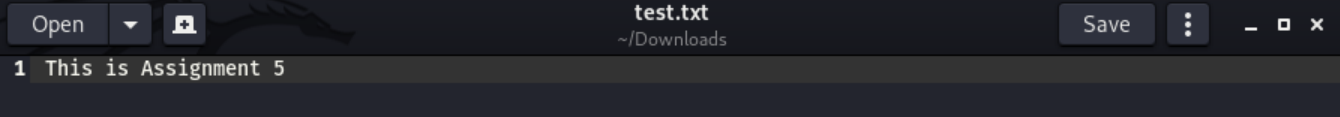
Description automatically generated

^Extracting any potential files that are additionally hidden using steghide.

A picture containing text, person, person, monitor

Description automatically generated

^Content of the first extracted data



^Contents of the final extracted data

Adding random numbers as a watermark to one of the extracted files



^Using convert to add the watermark towards the meme.jpg extracted file.

A picture containing text, person, person, monitor

Description automatically generated

^Final product where the .jpg file with the watermark is called memeKevin.jpg as the student number is 991602128.