Tracy Harvey

IS337

Module 10 Group Drop Box

1. No
2. The resolution/complexity of the cover medium (picture) matter to the amount of data you embedding in the image. The higher the resolution the more opportunities there are to embed data into it without making any noticeable differences from the original
3. Encrypting first would give the file that you embedded added security at the drawback of increasing the size file that you hid the message in by a noticeable margin. If you hide the message and then encrypt you get the benefit of reduced visibility it would be harder to detect the message but the trade off would be limited security. Both methods would increase the complexity of the operation because of having to decrypt and then extract the message instead of just having to extract the message.
4. Yes
5. Steghide (does not run natively on Mac but can with macPorts) <https://steghide.sourceforge.net>, SilentEye <https://achorein.github.io/silenteye/>, Steganography Studio <https://stegstudio.sourceforge.net/index.html>
6. Stegdetect <https://github.com/abeluck/stegdetect>, StegExpose <https://github.com/b3dk7/StegExpose>