**Lab Activity**

**“Steganography”**

**Part 1**

Read the article “[What is Steganography](https://docs.google.com/document/d/1xjHTmZw2Qt6dHuVBb-LqGnVaWjl6Z5dwohXxc0-sX3k/edit?usp=sharing)” and answer these questions.

1. **What is the advantage of steganography over encryption?** **(5 pts.)** An advantage of steganography over encryption is that it will conceal and encrypt data within digital content such as text, images, videos, audio, etc.; it aids in hiding the fact that there is sensitive data concealed.
2. **Give an example of how steganography has been used prior to the computer age.** **(5 pts.)** Before the computer age, steganography was used when people applied invisible ink in order to conceal confidential messages in otherwise inoffensive messages.
3. **What is watermarking and how is it used?** **(5 pts.)** Watermarking is considered to be a trademark that enables online publishers to recognize the source media files that have been distributed without any authorization or consent.
4. **Describe how Al-Qaeda used steganography.** **(10 pts.)** The Al-Qaeda used steganography by embedding hidden data on terrorist training videos and plans for imminent attacks in a pornographic video. This is an example of video steganography, which enabled them to insert concealed data into each frame of the video since it is a large file.
5. **How did a GE engineer use steganography to steal files**? **(10 pts.)** The GE engineer utilized steganography to steal files by taking data from 40 Matlab and Excel files. Then, he hid the stolen data in an image of a sunset by utilizing picture steganography techniques and emailed the image to themselves before sending the picture to their business partner based in China.
6. **Why aren’t MS Word files good for sending large amounts of data?** **(5 pts.)** MS word files are not a good option for sending large amounts of data because text files are typically small.
7. **How is hashing used to detect steganography?** **(5 pts.)** Hashing is used to detect steganography by taking the hash of the original file and then comparing it to the suspicious file. If the subsequent file is modified and there is concealed data in it, the hash will be different from the original file.

**Part 2**

Now you will get practice embedding images.  There are two browser-based tools that I have tested, and they do a reasonably good job of allowing someone to practice steganography:

* "Many Tools.org” - [Online Steganography tool (embed/hide secret messages or images within a host-image)](https://manytools.org/hacker-tools/steganography-encode-text-into-image/)
* "Image Steganography” - [Steganography Online - Encode message](https://stylesuxx.github.io/steganography/)

These tools use different encoding processes, and so images encoded with one cannot be decoded with the other.

1. **Use** [**Steganography Online (stylesuxx.github.io)**](https://stylesuxx.github.io/steganography/) **to encode a message into an image. Find an image online and hide some text in it. Upload the image to** [**Pasteboard**](https://pasteboard.co/)**, and put the link here. Pasteboard is the best option. However, if you cannot upload to Pasteboard, then rename your image with your name and upload it into** [**this folder**](https://drive.google.com/drive/folders/1FzU8vhSVESlqAgd8d_Z-YWHffiBEhEp-?usp=sharing) **(note, anyone with the link to this folder can edit. Just upload your file. Do not remove or modify the files of others).**  **(10 pts.)** <https://pasteboard.co/78PyWKLQJhKW.png>
2. Decode the image “[apple\_steg](https://drive.google.com/file/d/15l-QkB2Za5gbXbfbte4AhYdSvLWnSz3W/view?usp=sharing)”, and show you have decoded it with a screenshot of the decoded image. **(10 pts.)**

|  |
| --- |
| Graphical user interface, text, application  Description automatically generated |
| |  | | --- | | Graphical user interface, text, application  Description automatically generated | |

1. **You are working in a forensics lab.  You have been given some images to analyze (In the folder “**[**suspicious files**](https://drive.google.com/drive/folders/1CyJRLpICOf4IJh3a1LVJSb-nnXGXiSmA?usp=sharing)**”.)  The images seem harmless, as they were not encrypted, and it only seems to be primarily a bunch of frogs.  Check the images using the tools above. If you find nothing, then report this.  The images could be harmless.  If you find something, then summarize what you think is happening.  Draw some kind of conclusion and use the images as evidence for that conclusion. Your conclusion should be about 4 to 5 sentences.** **(35 pts.)** When I utilized the Steganography Online tool, stylesuxx.github.io to decrypt the message I found hidden messages embedded into each of the messages. For the partners.png file the hidden message *“Kasey - Deepdotweb has been seized by the popo. We need to find a new spot to get intel. Check it out -* [*https://www.deepdotweb.com*](https://www.deepdotweb.com)*”* . The frog\_key\_new.png file was also encoded with a message that showed an encrypted email that had information about a Bitcoin address. It showed the sender’s private and public key block. For the png files, avatar\_service.png, chocolate\_kasey1.png, frogger\_kasey2.png, kasey\_turnt\_headshot.png, novelty\_prices.png, toad\_terms.png, and tree\_basic.png I used the Online Steganography Tool, Many Tools.org. For avatar\_service.png, the hidden message is on personal information that is left blank on somebody’s CC/Cvv2 and the image chocolate\_kasey1.png’s message is about sending an order to Ms. Kasey. The next image frogger\_kasey2.png, has a concealed message that asks the sender about their location to ensure that they are not speaking to an officer and the image file kasey\_turnt\_headshot.png, is embedded with a message that has Black’s cloud URL. The image file novelty\_prices.png has purchasing information on the costs of four items hidden in the image, and the file toad\_terms.png has hidden information on payments and several discounts. Finally, the image file tree\_basic.png, has a hidden message about basic prices in the US and UK. In the images profane\_crypto, frog\_couple\_jpeg.jpeg, toy\_visa, and kermit\_kasey did not have embedded messages.



|  |
| --- |
|  |

A frog on a leaf

Description automatically generated with medium confidence

|  |
| --- |
| Graphical user interface, text, application  Description automatically generated |

|  |
| --- |
| A picture containing text, fabric  Description automatically generated |

|  |
| --- |
| Graphical user interface, text, application  Description automatically generated |

|  |
| --- |
| Graphical user interface, text, application  Description automatically generated |

|  |
| --- |
| A chocolate bar next to a box  Description automatically generated with low confidence |

|  |
| --- |
| Graphical user interface, text, application, chat or text message  Description automatically generated |

|  |
| --- |
| Graphical user interface, text, application  Description automatically generated |

|  |
| --- |
| A picture containing text  Description automatically generated |

|  |
| --- |
| Graphical user interface, text, application, chat or text message  Description automatically generated |

|  |
| --- |
| Graphical user interface, text, application, chat or text message  Description automatically generated |

|  |
| --- |
| A person with red hair  Description automatically generated with medium confidence |

|  |
| --- |
| Graphical user interface, text, application  Description automatically generated |

|  |
| --- |
| Graphical user interface, application  Description automatically generated |

|  |
| --- |
| A picture containing indoor, wall, green, frog  Description automatically generated |

|  |
| --- |
| Graphical user interface, text, application  Description automatically generated |

|  |
| --- |
| Graphical user interface, text, application  Description automatically generated |

|  |
| --- |
| A picture containing outdoor, tree, frog  Description automatically generated |

|  |
| --- |
| Graphical user interface, text, application, chat or text message  Description automatically generated |

|  |
| --- |
| Graphical user interface, text, application  Description automatically generated |

|  |
| --- |
| A picture containing frog, green  Description automatically generated |

|  |
| --- |
| Graphical user interface, text, application  Description automatically generated |

|  |
| --- |
| Graphical user interface, text, application  Description automatically generated |