Lab Activity

"Steganography"

Part 1

Read the article "What is Steganography" and answer these questions.

1. What is the advantage of steganography over encryption? **(5 pts.)** **It uses hidden text to hide the content whereas encryption is just jumbling the data.**
2. Give an example of how steganography has been used prior to the computer age. **(5 pts.)** **A secret message written with invisible ink.**
3. What is watermarking and how is it used? **(5 pts.)** **It's a trademark or other identifying data that's hidden in multimedia and is used to identify the source of media files that were shared without permission.**
4. Describe how Al-Qaeda used steganography. **(10 pts.)** **They hid Al-Qaeda documents including terrorist training manuals and plots for attacks within videos on flash drives and memory cards.**
5. How did a GE engineer use steganography to steal files? **(10 pts.)** **He hid Matlab and Excel files within an image of the sunset and emailed them to himself.**
6. Why aren't MS Word files good for sending large amounts of data? **(5 pts.)** **Because if the text is white, and the message is found by another person, they can highlight the text ad the plans are foiled.**
7. How is hashing used to detect steganography? **(5 pts.)** **All that needs to be done is just compare the hash of the altered file and the original file if possible.**

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)
- "Image Steganography" - Steganography Online - Encode message

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

8. Use Steganography Online (stylesuxx.github.io) to encode a message into an image. Find an image online and hide some text in it. Upload the image to Pasteboard, and put the link here. **(10 pts.)** **https://pasteboard.co/W13A1ekD4xZe.png**
9. Decode the image "apple_steg", and show you have decoded it with a screenshot of the decoded image. **(10 pts.)**

10. You are working in a forensics lab. You have been given some images to analyze (In the folder "suspicious files".) The images seem harmless, as they were not encrypted, and it only seems to be primair 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. The images are in the lab folder. **(35 pts.)**

Some of the messages are for bitcoin transfer between two users with credit cards, with one user telling the other to speak with Ms. Kasey and then Rozzer Black. They were found out first on the first website they were using and moved to a different site. Some of the images state prices given with the cards with CC/Cvv2 information on them.