**Lab Report**

**Lab Completed: Steghide**

**Objective:** Complete the lab presented. Using your textbook, the written lab, and the hands-on activity, use the lab report to demonstrate understanding of the concept presented.

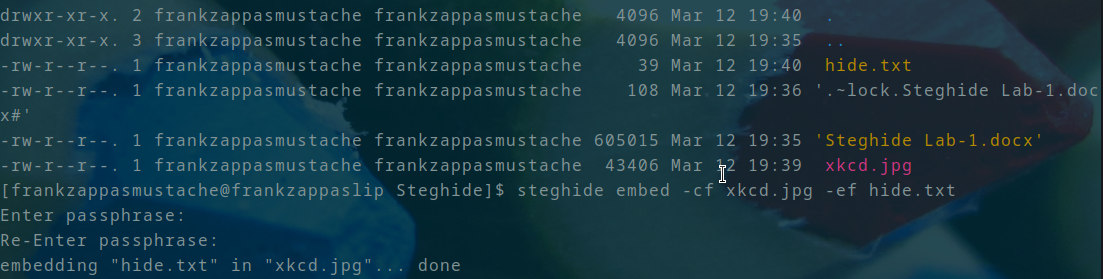
**Part 1: Lab Activity**

Directions: Complete the lab assigned in Netlab. Take 2 screenshots (or more) that demonstrate completion of the lab. Answer the following:

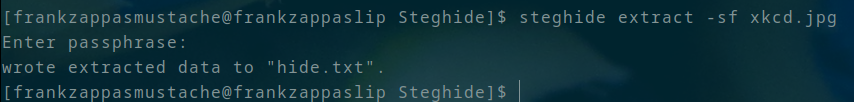
**Q1:** Provide a synthesis of the activity you completed in your own words.

In this lab we embedded text in an image file and then extracted that same text using steghide.

**Q2:** Provide 2 screenshots that demonstrate lab completion. For each screenshot, include 1-2 sentences explaining what the screenshot is demonstrating.



Here I was using steghide to embed the contents of text document hide.txt into the image xkcd.jpg



Here I was extracting the embedded text from xkcd.jpg using steghide.

**Part 2: Critical Thinking**

**Directions**: Complete the following questions. Provide an explanation of your reasoning for each answer.

The answers should address the lab you just completed.

Suggested length for Part 2: 1-2 pages

**Q1**: What vulnerability(s) are demonstrated or found in this lab? Vulnerabilities may occur during the lab as part of the lab activity.

There were not really any vulnerabilities present during this lab activity.

**Q2:** How might this (these) attack(s) be utilized during a penetration test?

One could use image files with steghide to bring information into or out of an organization without seeming conspicuous.

**Q3:** Explain your reasoning as to what phase of the attacker methodology this lab falls under.

If this were to be used, it would probably be in the exfiltration phase

**Q4:** Research how the attack(s) in this lab can be mitigated or prevented. Cite any sources used. (APA)

One could use some kind of iDS/IPS to flag the use of steghide and log it. You might also use file checksums to identify when the file has been changed, but I don’t know how much use that would be considering an image file might be edited and it’s checksum changed for a number of reasons.

**Q5:** What ethical or potentially problematic issues should a penetration tester consider if they plan on implementing this (these) attack(s) by exploiting a vulnerability?

They may want to make sure any information they are introducing to the network or exfiltrating from the network is removed afterward.