Steps to Complete the Challenge:

1) Took a picture of the given paper filled with binary. Ran the picture through brandfolder website to convert the picture into text. Then we ran that text through rapidtables website to convert the binary to readable text. The text was:

   FTP at 138.47.99.228 - port 21 - user is salt - pass is saltXXXXY - where XXXX is a TimeLock code and Y is the last character of the final TimeLock hash - TimeLock epoch is 2023-11-03 00:00:00 - sync your time using telnet or netcat on port 54321

2) Then we telnet into the server and found the current time is just the current system time. We found the password from running program5 to get the first four digits and then the last digit came from the last character of the hash code after the second time it was hashed.

3) Then once we got into the server using the username salt and password saltad616, turned the passive mode on and then ran the ls -l to see a bunch of files. We downloaded the files using the command mget *

4) After downloading the files, we looked through the files and found that they are all images but one of the images had some noise in it.

5) We used the steg file to decode the file with the options: python steg_01.py -r -B -o 262144 -i32 -w <filename> and then output the results into a file called ouput

6) The message said ignore everything that's not binary and then the binary showed up so we ran the binary into a binary to ascii to get the clue.

7) The clue said:

   A cipher that starts with a V. Use it as a key to help you! Bw hepo ksA_aVAMeWueSciVAETAWYIBASY]aGSS_VACmqrAruW[mielANuiuqmSJ\@A1sSRA_ WpAOYlAQukkeLAgYp

8) Then we used the vigenere program to to decode the message

9) The message said to login into the ftp server with the username and password of pepper to get the demons out.

10) Once logged in there were 2 more files that we downloaded.

11) After getting those 2 files, we used our XOR program to decode the message which stated that we had to login into the server again with username and password garlicpowder

12) Once we logged in again, there was another file that we downloaded.

13) This file said we had to find out what the smallest fish in the world was and then tell the professor. The final answer is Paedocypris progenetica

Contributions:

Kaylee: I helped with getting the password to get into the server the first time as well as finding the clues hidden in each picture.

Andrew: Ran the steg file more than I would like to admit, logged into ftp to grab demon files and conclusion file, and ran xor on demon files. Looked up weird fish name

Tommy: Synced my computer time using telnet. Once we got the password for the ftp server, I grabbed the images. I decode the vignere cipher for the second user and password for ftp server and grabbed the demon files.

John: Helped in the ftp server. Also did exploit research for the elite port

Hayden: I helped find the password to get into the ftp server and identified which picture needed to be targeted by our steganography program.

Tim: Converted binary page to ascii. Pulled pictures from FTP. Got the current system time to use using Telnet.

Gabe: I first got the epoch time from doing telnet on the IP address and port given from the binary we were given on paper. Using that we got the password for the ftp where I then logged in and tried to get the files needed for the rest of the code. We then used our steg code in order to decipher the bmp files we got from the ftp server.