**Clues From pcap “TheEnd”**

**PCAP Link:** <https://drive.google.com/file/d/1LTBBqKsF1NDthrQf7Gr0ggWoLQ9JnNj_/view?usp=sharing>

1. From the packets #632 and #633(found by Tanushri), a Github.io link was found associated with the username vicog24
2. After logging into Github, a link with source code for a website was found --- <https://github.com/vicog24/TheEnd/blob/main/SignInCheck.js>
3. Adding to the vicog24.github.io link that was found in the pcap file with a forward slash to access the specific “TheEnd”(as per both the Github repository and the title of the pcap file) page, the following link was typed into the browser: <https://vicog24.github.io/TheEnd/>

* Takes you to “Espacio X”(Pelon’s company)
* Asks for username and password, which were obtained from examining the source code from the first Github page
  + Entered the following:
    - Username: “Expect\_Us”
    - Password: “W3\_@r3\_n@m3l3$$”
    - Determined because:
      * Source code on the Github page read as follows, meaning that the username and password from above were the correct ones because they would lead to another page on the site:

if(loginForm.uname.value=="Expect\_Us"){

if(loginForm.psw.value=="W3\_@r3\_n@m3l3$$")

{

location="page2.html";

}

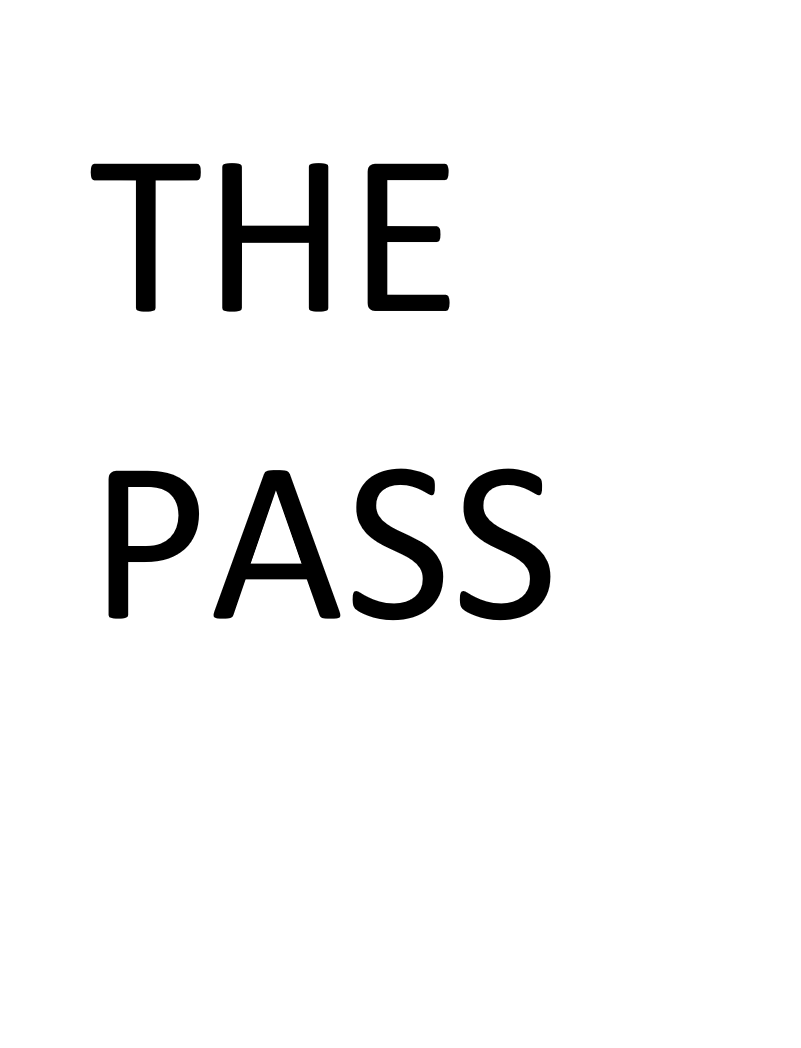
1. The page displayed following successful login displayed the 2 following links:
   1. [Finale.zip / https://drive.google.com/file/d/1igoSO2z4f3ubZz3CcvCLqQoZp-hU6V0e/view](https://drive.google.com/file/d/1igoSO2z4f3ubZz3CcvCLqQoZp-hU6V0e/view)
   2. [Desktop.zip](https://drive.google.com/file/d/1ALEir2iJd3_aMke26jCMdyDAb60qGDw_/view) [/](https://drive.google.com/file/d/1igoSO2z4f3ubZz3CcvCLqQoZp-hU6V0e/view)

<https://drive.google.com/file/d/1ALEir2iJd3_aMke26jCMdyDAb60qGDw_/view>

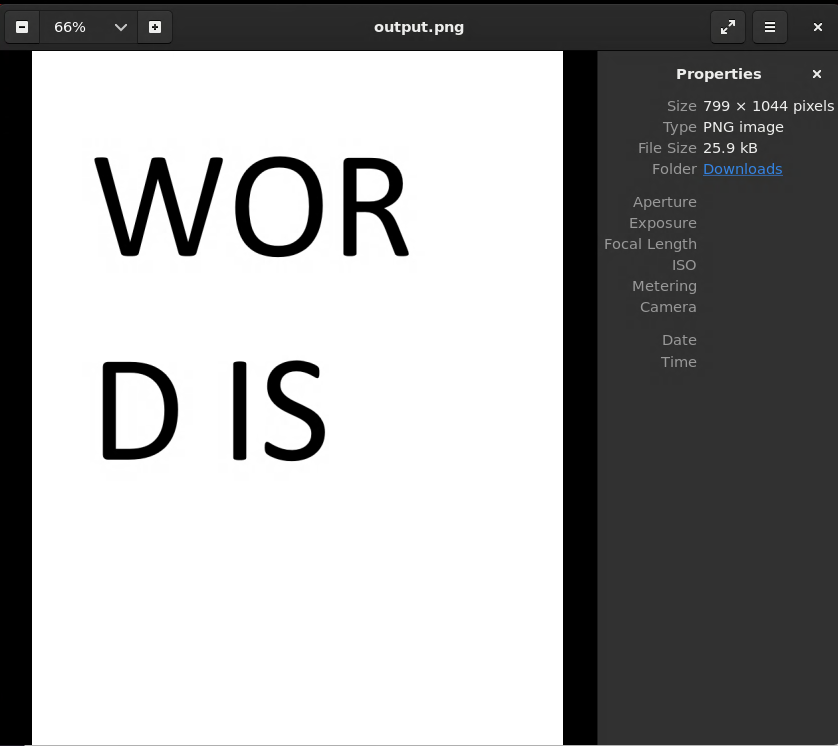
* 1. The contents of both of these links are password protected

***Getting the Passwords***

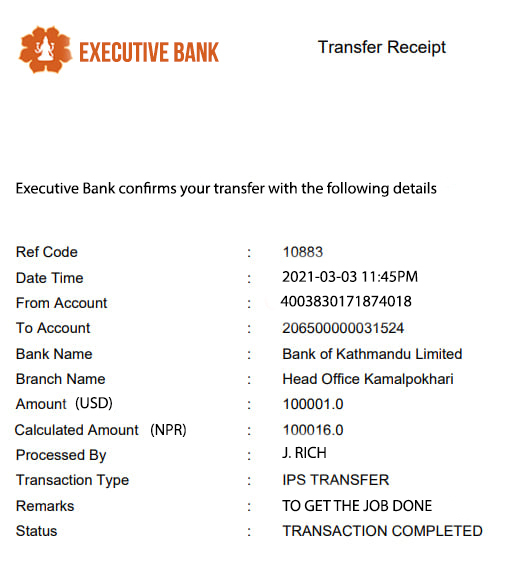
1. Password for Desktop.zip: **Mars** 
   1. Determined using John the Ripper,
      1. first ran: zip2john Desktop.zip > hash.txt command to save the hash in a text file
      2. then ran: john --format = PKZIP hash.txt command to actually crack the password
   2. Link to cracked, unzipped Desktop:
      1. <https://drive.google.com/drive/folders/18gEgDDRJhWBKLN6CHeaR8yzVr7FgdC90?usp=sharing>
      2. From desktop, three images were obtained and run through steganography programs to find hidden messages:
         1. Image 1: After running Image1.png through Digital Invisible Ink Toolkit using the BattleSteg algorithm, a hidden PNG image was found, saying THE PASS



* + - 1. Image 2: After running Image2.png on the DIIT using the DynamicBattleSteg algorithm, the hidden PNG image was found, saying WORD IS



* + - 1. Image 3: After running Image3.png on the DIIT using the Hideseek Algorithm, the hidden png file was found stating “SP@C3FL1GH7”



1. Password for Finale.zip: **SP@C3FL1GH7**
   1. There were two attachments within the zip file:
      1. Receiptcopy.jpg:
         1. Shows J. RICH(most likely Rich Brandad) as having transferred money to “get the job done”
      2. Finale.txt: Voe Ukjh dndabu diq.....
         1. This is a vigenere cipher with key CHAD and is decrypted as: The Rich always win… showing that Rich Brandad is the one that is responsible.

**Final Conclusion: RICH BRANDAD was responsible**