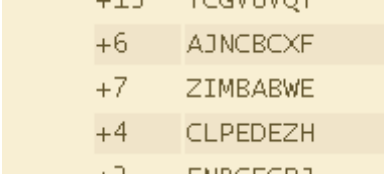
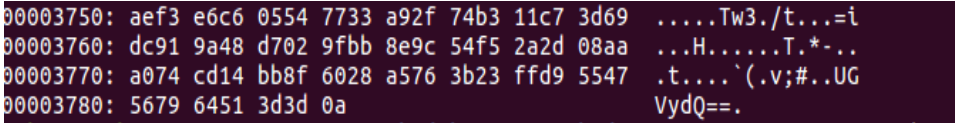
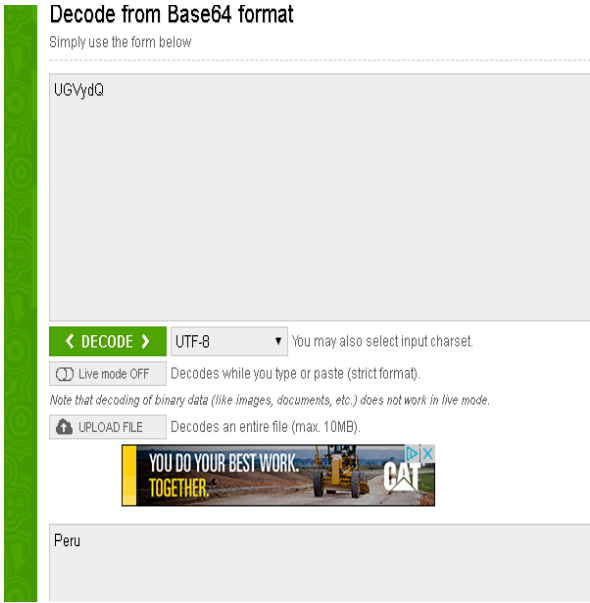


## Laboratory Notes

Laboratory Number: \_\_\_\_4\_\_\_\_

Examiner Name: Kelli Kinnikin

Date & Time	Activity
12/4/17 3:00 p.m	<p>Before I could do this lab, I had to download multiple sources/tools.</p> <ul style="list-style-type: none"> <li>• Command: “ sudo apt-get install steghide”</li> <li>• Command: “sudo apt-get install python-progressbar</li> <li>• \$gitclone <a href="https://github.com/Va5c0/Steghide-Brute-Force-Tool.git">https://github.com/Va5c0/Steghide-Brute-Force-Tool.git</a></li> <li>• Command: “scp <a href="mailto:cis425@mathcs.wcfontbonne.edu">cis425@mathcs.wcfontbonne.edu</a>:~/Lab4.tar ./”</li> </ul>
12/4/17 3:06 p.m	<p>After downloading all those previous sources/tools, I ran the steghide-brute-force-tool and inserted the 1st jpg image into the tool.</p> <pre> Lab4          mystery-flag-3.jpg  steg_brute.py LICENSE       mystery-flag-4.jpg  wordlist.txt mystery-flag-1.jpg  mystery-flag-5.jpg mystery-flag-2.jpg  README.md python steg_brute.py -b -d wordlist.txt -f mystery-flag-1.jpg  [i] Searching... 98% #####   wrote extracted data to "mystery-flag-1_flag.txt".  [+] Information obtained with password:  the flag is {Denmark} </pre> <ul style="list-style-type: none"> <li>• Wordlist.txt was given to me in the .tar file</li> <li>• FLAG: {Denmark}</li> </ul>
12/4/17 3:20 p.m	<p>Next, I placed the 2nd jpg image into the brute force tool.</p> <pre> python steg_brute.py -b -d wordlist.txt -f mystery-flag-2.jpg  [i] Searching... ##### Amazon wrote extracted data to "mystery-flag-2_flag.txt".  [+] Information obtained with password: Thailand2017  The flag is {Thailand} </pre> <ul style="list-style-type: none"> <li>• FLAG: {Thailand}</li> </ul>
12/4/17 10:03 p.m	<p>This time I used the “xxd” command to find the hidden message.</p> <pre> 00006680: 7bdf baf7 5ef7 eebd d7bd fbaf 75ef 7eeb {...^.....U.~ 00006690: dd7b dfba f75e f7ee bdd7 bdfb af75 ef7e {...^.....U.~ 000066a0: ebbd 7bdf baf7 5ef7 eebd d7bd fbaf 75ef {...^.....U.~ 000066b0: 7eeb dd7b dfba f75e f7ee bdd7 bdfb af75 ~..{...^.....U 000066c0: ef7e ebbd 7bdf baf7 5ef7 eebd d7ff d954 ~..{...^.....T 000066d0: 4845 2066 6c61 6720 6973 207b 5375 6461 HE flag is {Suda 000066e0: 6e7d 0a </pre> <ul style="list-style-type: none"> <li>• FLAG: {Sudan}</li> </ul>

<p>12/4/17 10:26 p.m</p>	<p>To get the 4<sup>th</sup> flag I used the command:</p> <ul style="list-style-type: none"> <li>• Command: “xxd”</li> <li>• The message was encrypted, so I used a Caesar cipher online tool to decrypt it</li> </ul>  <ul style="list-style-type: none"> <li>• FLAG: ZIMBABWE</li> </ul>
<p>12/4/17 10:30 p.m</p>	<p>To get the mystery-flag-5.jpg, I used the “xxd” command again along with a base64 decoder.</p> <ul style="list-style-type: none"> <li>• The “UGVydQ” is what goes into the online decoder tool</li> <li>• FLAG: Peru</li> </ul> 
<p>12/4/17 10:33 p.m</p>	

--	--