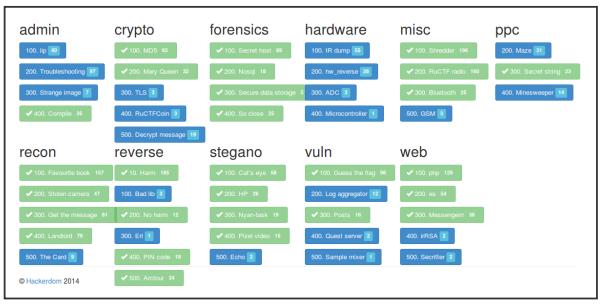
EVERLASTING WANDERER

SETTING OUT ON A NEW JOURNEY TO FIND THE MEANING OF LIFE...

MONDAY, MARCH 10, 2014

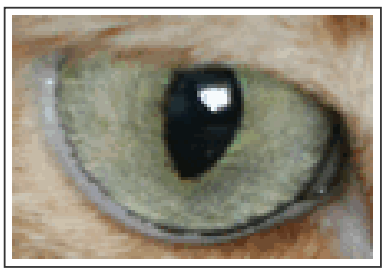
RuCTF Quals 2014

Another great CTF with many challenges in all categories just ended. Our team was #7. Nana. Not too bad, but it was so annoying that without a network specialist we could not solve admin 200 task "Troubleshooting" which 97 other teams solved with ease.

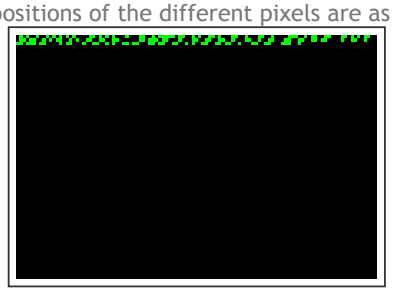


Below are some write-ups. Hopefully they can give new players an introduction to steganalysis.

stegano 100: Cat's eye



This is an easy GIF stegano, but it took me quite a while analysing the image until I noticed it contained 8 similar frames which wasn't easy to notice in GIMP by default (note to myself: next time check the frames first). It is common sense to combine them and find the differences. The positions of the different pixels are as marked below:



It isn't very straightforward, but the flag is hidden here in binary representation. Using black pixels as 0s and green pixels as 1s give you the
flag: RUCTF_e4dd9f5cee307b322c3a27abe66e3df9

stegano 300: Nyan-task

ABOUT ME

QUANGNTENEMY

HANOI, VIETNAM

A young tiger & penguin tamer who has special interest in computer-based challenges, especially The Black Sheep at http://www.bright-shadows.net. On his journey to find the meaning of life!

VIEW MY COMPLETE PROFILE

TWITTER UPDATES

MY SITES

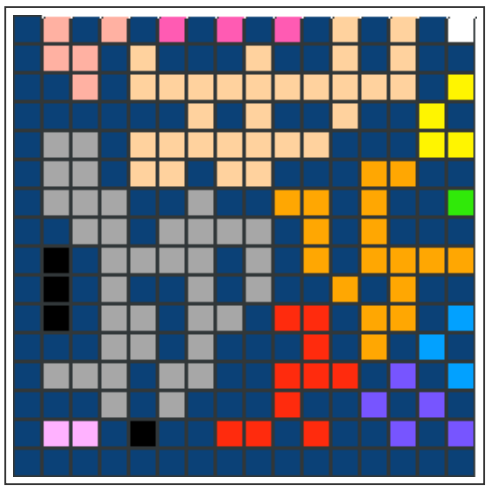
Homepage
Penguin Tamer
quangntenemy teaches Java
WeChall

MY NETWORK

Alt3rn4tiv3's Tech Blog
Bb's blog
Chaotic Dreams
Inferno's blog
Paralax's blog
Rankk's blog

BLOG ARCHIVE

This is a very famous image. By finding and comparing it with the original image it can be concluded that there is no information hidden visually. Analysis with Caesum's StegSolve brought me to the conclusion that the only place to hide the flag is inside the palette. It is also suspicious to see only 14 colors used for the image while the palette contains 256 colors with a lot of repetition.



After extracting the palette I found out that this is actually a DataMatrix barcode (thanks stypr). The rest is easy. The hidden text is u.to/P4JUBg, which is a link to the flag: RUCTF_ca8250c2b4b50581afc9ffd1f403f3f2

crypto 200: Mary Queen

The task is to decipher a message written in Chinese characters. The title suggests that this is similar to the cipher used by Mary Queen of Scots, which is a cryptosystem in which simple substitution is used. This cipher is so weak that many tools have been created to solve it automatically, SCBSolvr is one of them. The decrypted text is chapter I of Alice's Adventures in Wonderlands by Lewis Carroll. The name of the book is also the flag.

POSTED BY QUANGNTENEMY AT 3:24 PM

LABELS: 2014, CRYPTO, CTF, RUCTF, STEGANO

NO COMMENTS:

Post a Comment

Newer Post Home Older Post

► 2013 (2)
► 2012 (1)
► 2011 (1)
► 2010 (7)
► 2009 (5)
► 2008 (21)
► 2007 (59)

SEARCH THIS BLOG

Search

LABEL CLOUD

2007 2008 2014 2038 java steganabara mandriva bbq ctf qtj rankk stegano message me tutorial ubuntu applet freerice jbb linux spring 2008.1 bot cryptobox rpg security urpmi website 2009.0 challenge concurrency gnome homepage host irc kde kde4 microsoft minesweeper object oriented virus vpn wechall xss .net 0x3004 10.04 2009.1 2010.0 AccessFlags DotA Friday the 13th HTTP Error 403.2 New7Wonders TLFG all the strings alsa arts asis backtrack bootloader caesum calendar cat chamber door checksum chess cloud computing codeproject collision copy crackit crypto css cvs dashfer defcon font forumwarz gdm greasemonkey hacking hackquest ibm idlemonkeys iis interview iso jackpot jad jmine jquery jsf juniper kernel kvirc lucid lynx mcafee md5sum metabase mp3 ohloh olympic open source opera partition password phdays pidgin ping problem prototype proxomitron qmine quangnitron rating reflector reflexil reverse engineering rpm ructf sendmail service sha1sum siteadvisor smashthestack solaris spam poison split sql injection swap table-less tbs technorati theblacksheep thehivemind tomahawk trusty tweak unxutils update vietnam wargame

wikipedia xml challenge xorg.conf
xssed zip