HACKFEST COMMUNICATION

SOLUTIONS / SOLUTIONNAIRE

DISCOUNT CODES / COUPONS RABAIS
HACKFEST.CA 2012

Disclaimer

Discount codes are disabled, but you can still play the game and find all 4 codes, or cheat and look at the answers in the next few pages :)

05$:View source

- Go to www.hackfest.ca/hacking-games
- View-source
- Find: Code 5$ discount (looks like an md5 hash)
- Enter the code and you got 5$ discount

10$: QR Code

- There are 4 images to find on the Hackfest websites
  - Hackfest.ca has 2
  - Flickr.com has 1
  - Facebook.com has 1

QR Code : step 1

- Go to www.hackfest.ca/formation-2
- View source
- Find: <!-- TITANIC IMAGE: /img/supertitanic l ofour.jpg -->
- Get image!

QR Code : step 2

- Go to www.hackfest.ca/robots.txt
- find:
  Disallow: /asdqwe123.jpg #titanicXof4.jpg
- get image!

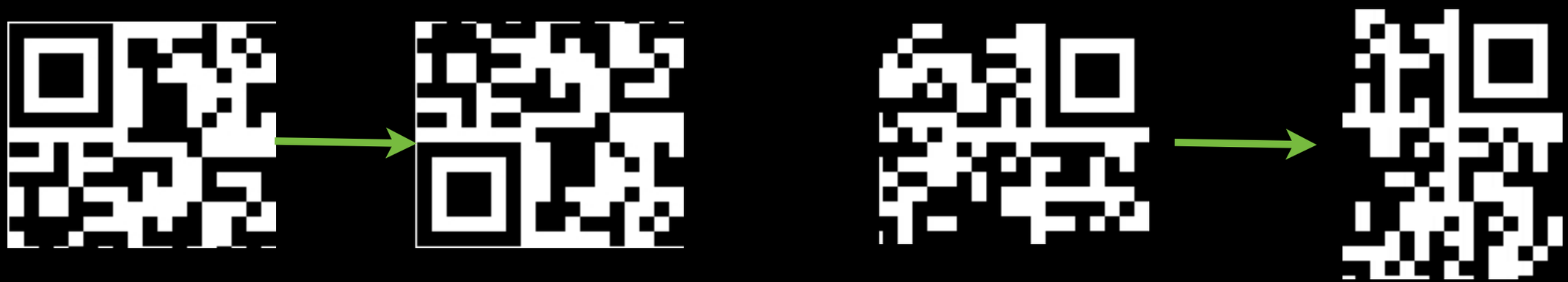
QR Code : step 3

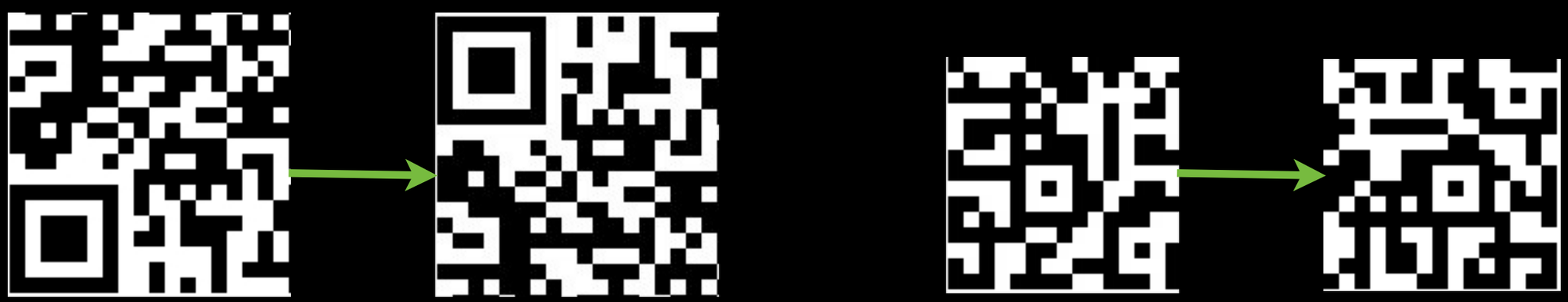
- Go to flickr.com/photos/hackfest2k9
- go to page 30th or so
- Get image!

QR Code : step 4

- Go to www.facebook.com/hackfest
- Go to our image section and find a QR code part
- Get image!

QR Code : step 5
Moving the parts





QR CODE : STEP 6

- Reassemble, scan and get 20$ discount!
- *This background colour will help the scanner app to scan! :)

15$: Exiftool

- This is simple but long and “boring”
- Download all image of the website with wget -R ... and then do an exiftool on all of them!
- The image “Powered By Hackfest” Got a message saying “No discount code here”
- But the WallPaper “official-1900.jpg” has the 15$ discount code in the comment exif field.

20$: Steghide

- The clue that was given : “The password is in the most viewable image”, which is the logo of our website! We see it first on the website and it is on every page. Compare to black.jpg which is on every page but we don’t “see” it.
- The logo got 3 specials elements
  - A Copper battery
  - Word “Revolution”
  - Sentence: “Welcome to the real world” (http://youtu.be/TrhRzxoFH-4)
- Those 3 are from the Matrix movies.
- The Copper battery is in the scene where the real world is explain (http://youtu.be/tiS7sCcSLUQ)
- Simply google the sentence and you see this has been said by Morpheus.
- Password = morpheus

Invalid 15$ and 20$ code?

- Yeah right finding an exif is easy and you think it was over?
- Registration discount code field got a 25 max length.
- You have to use BurpProxy or any other tool to push the 32 characters long md5 into the 25 long field.