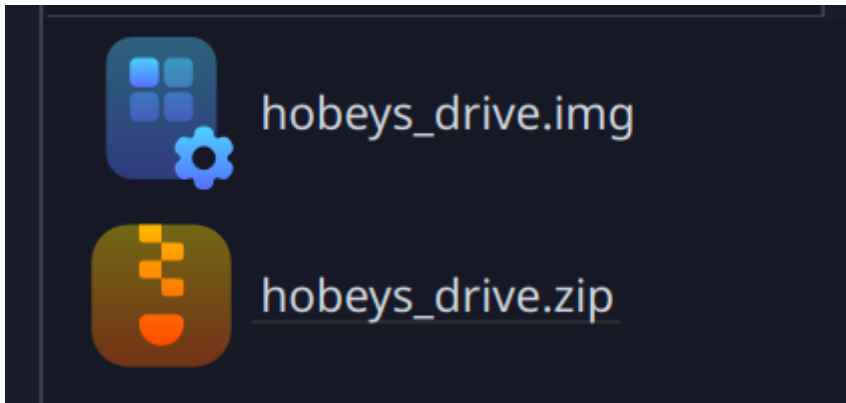


# Where is the solution?

Mark Grünzweil, 3 AHIF, 06.12.2024

## Lösung

Herunterladen der Anfangsdatei



Benutzen von Testdisk um die Datei zu bekommen

```
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
```

```
TestDisk is free software, and
comes with ABSOLUTELY NO WARRANTY.
```

```
Select a media and choose 'Proceed' using arrow keys:
```

```
>Disk hobeys_drive.img - 1048 KB / 1024 KiB
```

```
>[Proceed ] [ Sudo ] [ Quit ]
```

```
Note: Some disks won't appear unless you are root user.
```

```
Disk capacity must be correctly detected for a successful recovery.
```

```
If a disk listed above has an incorrect size, check HD jumper settings and BIOS
detection, and install the latest OS patches and disk drivers.
```

TestDisk 7.2, Data Recovery Utility, February 2024  
Christophe GRENIER <grenier@cgsecurity.org>  
<https://www.cgsecurity.org>

Disk hobeys\_drive.img - 1048 KB / 1024 KiB - CHS 64 2 16

Partition	Start	End	Size in sectors
> P FAT12	0 0 1 63	1 16	2048 [STARDUST]

[ Type ] [ Boot ] >[Undelete] [Image Creation] [ Quit ]  
File undelete

TestDisk 7.2, Data Recovery Utility, February 2024  
Christophe GRENIER <grenier@cgsecurity.org>  
<https://www.cgsecurity.org>

P FAT12 0 0 1 63 1 16 2048 [STARDUST]  
Directory /

>-rwxr-xr-x	0	0	399000	16-Jun-2021	12:21	my_holiday_destination.jpg
-rwxr-xr-x	0	0	742	16-Jun-2021	08:21	my_passwords.base64
-rwxr-xr-x	0	0	850	15-Jun-2021	19:22	for_james.zip
-rwxr-xr-x	0	0	84101	16-Jun-2021	12:32	instructions_for_james.pdf

Next

Use **Right** to change directory, '**h**' to hide deleted files  
'**q**' to quit, ':' to select the current file, '**a**' to select all files  
'**C**' to copy the selected files, '**c**' to copy the current file

```
~/Downloads/NSCS/Image > ll
total 1.5M
-rw-r--r-- 1 mark mark 850 Jun 15 2021 for_james.zip
-rw-r--r-- 1 mark mark 1.0M Jun 16 2021 hobey's_drive.img
-rw-r--r-- 1 mark mark 83K Jun 16 2021 instructions_for_james.pdf
-rw-r--r-- 1 mark mark 390K Jun 16 2021 my_holiday_destination.jpg
-rw-r--r-- 1 mark mark 742 Jun 16 2021 my_passwords.base64
~/Downloads/NSCS/Image > █
```

## Lesen der PDF Datei 'Instructions\_for\_James.pdf'

Dear James,

I've decided to hide my messages inside images. It's called steganography.

Every time I record one of my messages, it will be automatically embedded in an image and uploaded to our server.

Genius, I know.

Here's what you do after downloading the image:

1. Go to <https://stegonline.georgeom.net>.
2. Upload the image.
3. Select "Extract Files/Data".
4. Set exactly the bits in the table shown below.
5. Click "Go".

I'll send you the links to the images as an encrypted QR code. You already know the password, it's our favorite line of the best song ever.

This is foolproof. We're going to be very rich, very soon.

Best,  
David

## Auf **StegOnline** gehen und die Datei hochladen

StegOnline

Upload

CTF Checklist

About

---

UPLOAD IMAGE

Drag and drop your image here

***Back to Home***

## Extract Data

Here you can extract data hidden inside of the image. Select some bits and adjust the settings appropriately. The final extracted data is checked against some basic file headers, and so the filetype can be automatically determined.

Please note that Alpha options are only available if the image contains transparency.

	R	G	B
7	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

## Pixel Order

Row 

## Bit Order

MSB 

## Bit Plane Order

R v G v B v

## Trim Trailing Bits

No ▾

Go

## Results

*No file types identified.*

The results below only show the first 2500 bytes. Select "Download" to obtain the full data.

Ascii (readable only):

.....	.....	.....	.....	.....	.....	.....
.....	.....	.....	.....	.....	.....	.....
.....	.....	.....	.....	.....	.....	.....

Hex (Accurate):

```
f6f6f6f6f5f5f5f5f6f6f6f6f6f6f6f6f6f6f6f6f6f6f6f6f5f5f5f5f5f6f0f4f
7f8f5f5f6f8f5f6f6f7f7f6f6f5f6f6f6f6f5f5f5f5f6f6f6f6f6f6f6f6f5f5f5f5f6
f6f6f6f5f5f5f5f5f5f5f5f6f6f6f7f7f8f8f8f7f7f6f6f5f5f5f5f5f6f6f6f6f6f6f6f
```

Download Extracted Data



my\_holiday\_destination.dat

**Note:** Die Datei ist komplett sinnlos und hat keinen wertvollen Inhalt für die Lösung.

## Decoden der Base64 Datei



Base64 Decode


<https://www.base64decode.org>

### Base64 Decode and Encode - Online

Decode from Base64 format or encode into it with various advanced options. Our site has an easy to use online tool to convert your data.

#### Decode files from Base64 format

Select a file to upload and process, then you can download the decoded result.

 Click (or tap) here to select a file

1

 The maximum file size is 192MB.

 Do not execute decoded files originated from untrusted sources.

☐ Decode each line separately (useful for when you have multiple entries).

< DECODE >

✓ Success!

CLICK OR TAP HERE to download the decoded file.

Please note that this file is removed from our system immediately after the first download attempt or 15 minutes of inactivity.



decoded-20241213073820.txt

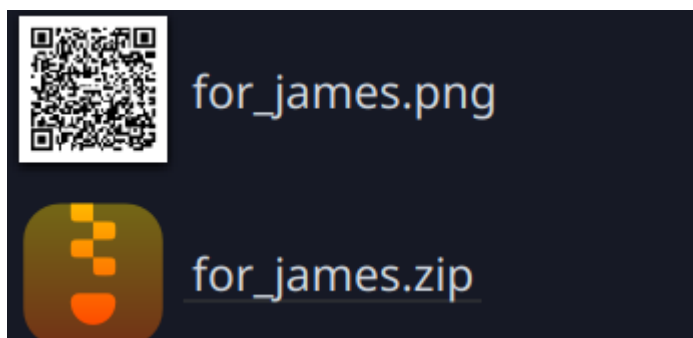
## Inhalt der Datei:

PASSWORD	DESCRIPTION
We can be heroes, just for one day	QR codes for James
Life on Mars?	Twitter
Ground control to Major Tom	SoundCloud

## Den Verschlüsselten Zip Ordner decoden

Passwort: We can be heroes, just for one day

We can be heroes, just for one day | QR codes for James



## Den QR-Code scannen



[https://share.mb.sb/teaching/forensics/challenges/where\\_is\\_the\\_money/where\\_is\\_the\\_money.png](https://share.mb.sb/teaching/forensics/challenges/where_is_the_money/where_is_the_money.png)

Auf dieser Website das Bild herunterladen





Dieses Bild wieder auf [StegOnline](#) hochladen

UPLOAD IMAGE

Drag and drop your image here

[Back to Home](#)

## Extract Data

Here you can extract data hidden inside of the image. Select some bits and adjust the settings appropriately. The final extracted data is checked against some basic file headers, and so the filetype can be automatically determined.

Please note that Alpha options are only available if the image contains transparency.

	R	G	B
7	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Pixel Order

Row ▾

Bit Order

MSB ▾

Bit Plane Order

R ▾ G ▾ B ▾

Trim Trailing Bits

No ▾

Go



## Results

## Identified Filetypes

mp3: MP3 file with an ID3v2 container

The results below only show the first 2500 bytes. Select "Download" to obtain the full data.

Ascii (readable only):

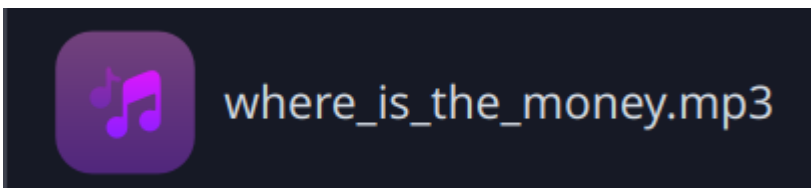
```
ID3..@..  .=.....  ..HSvyTI T2.....  .Message    to Jame  sTPE1...
....Davi d HobeY.  ..D.....  .....  .....  ...Xing.
.....V.  ..X.....  .....  . #&)+- /  146:<>@C  EHKMPRUW  Y[_acehj
```

Hex (Accurate):

```
4944330400400000003d0000000c012005004853767954495432000000110000004d6  
5737361676520746f204a616d6573545045310000000c000000446176696420486f62  
6579fffb904400000000000000000000000000000000000000000000000000000000
```

Download Extracted Data

## Downloaden der Datei



## Den Sound anhören

Beim Anhören kann man der er das Geld hier versteckt hat:

Westmansterstreet 14, behind the trashcan